NOTE TO USERS

UNIVERSITÉ DE MONTRÉAL

ARCHITECTURE DE SÉCURITÉ POUR ENVIRONNEMENT D'APPRENTISSAGE MOBILE

GAËL TEXIER
DÉPARTEMENT DE GÉNIE INFORMATIQUE
ÉCOLE POLYTECHNIQUE DE MONTRÉAL

MÉMOIRE PRÉSENTÉ EN VUE DE L'OBTENTION
DU DIPLÔME DE MAÎTRISE ÈS SCIENCES APPLIQUÉES
(GÉNIE INFORMATIQUE)
NOVEMBRE 2004

Your file Votre référence
ISBN: 0-494-03920-5
Our file Notre référence
ISBN: 0-494-03920-5

UNIVERSITÉ DE MONTRÉAL

ÉCOLE POLYTECHNIQUE DE MONTRÉAL

CE MÉMOIRE INTITULÉ :

ARCHITECTURE DE SÉCURITÉ POUR ENVIRONNEMENT D'APPRENTISSAGE MOBILE

présenté par : TEXIER, Gaël
en vue de l'obtention du diplôme de : maîtrise ès sciences appliquées
a été dûement accepté par le jury d'examen composé de:

M. GAGNON Michel, Ph. D., président
M. PIERRE Samuel, Ph. D., membre et directeur de recherche
M. QUINTERO, Alejandro, Doct., membre et codirecteur de recherche
M. BOUDREAULT Yves, M.Sc., membre

À ma famille

REMERCIEMENTS

Je remercie sincèrement mon Directeur de recherche M. Samuel Pierre pour son encadrement, ses précieux conseils ainsi que son support moral et financier tout au long de mes recherches au sein du LARIM.

Je tiens aussi à remercier mon codirecteur, le professeur Alejandro Quintero pour sa disponibilité, sa patience et ses commentaires tout au long de ce projet.

Merci également à ma famille qui m'ont toujours encouragée et soutenue pendant ma maîtrise. Mes remerciements vont ensuite à tous les membres du LARIM qui ont toujours été disponibles pour m'aider, particulièrement M. Marc Doyon, Mme Betty Momplaisir et Mme Sabine Kébreau.

RÉSUMÉ

Actuellement, les établissements d'enseignement ne peuvent se permettre d'évaluer les étudiants suivant un cours sur Internet, étant donné la faible sécurité de cet environnement. Les établissements désirent obtenir la note de crédibilité la plus élevée possible et ceci débute par la manière d'évaluer les étudiants. Les universités doivent inévitablement sécuriser leurs environnements d'apprentissage afin d'offrir l'éducation à distance dans les meilleures conditions. Les deux principaux problèmes des environnements d'apprentissage virtuel actuels sont : la faible sécurité et l'impossibilité d'accéder à l'environnement par appareils mobiles.

Avec les appareils mobiles maintenant disponibles sur le marché pour accéder à Internet, il est indispensable de donner la possibilité aux étudiants de les utiliser afin qu'ils puissent accéder à l'environnement d'apprentissage virtuel, sans toutefois négliger la sécurité. L'amélioration de la qualité de l'éducation et de l'apprentissage doit reposer sur un environnement sécuritaire, peu importe l'utilisation du médium, en offrant une qualité de service satisfaisante et en permettant la mobilité de la personne, du terminal et des services.

La mobilité lors d'apprentissage virtuel pose inévitablement un problème de sécurité, très différent de la sécurité dans les environnements câblés. Dans ce mémoire, nous nous sommes intéressés à l'environnement d'apprentissage virtuel mobile ainsi qu'à la sécurité reliée à ce milieu. Comme le *m-learning* possède ses problèmes spécifiques de sécurité, nous les traitons distinctement afin de comprendre et proposer une solution adéquate. Nous portons également un regard sur les architectures d'apprentissage virtuel actuelles et nous proposons une architecture sécuritaire pour un environnement d'apprentissage mobile de type laboratoire virtuel. Finalement, nous évaluons la performance de notre architecture.

Nous avons conçu une architecture sécuritaire dans un environnement d'apprentissage virtuel et mobile. Afin de tester notre modèle nous avons simulé des usagers dans un réseau filiaire et un réseau WLAN. L'idée principale était de comparer la performance de notre architecture à une architecture semblable sans sécurité.

Les simulations menées dans l'environnement WLAN ont montré que les mécanismes de sécurité utilisés constituent un coût raisonnable à payer afin d'assurer la sécurité dans un environnement d'apprentissage. Des mesures de performance nous ont également permis de quantifier le coût de l'utilisation du mécanisme de sécurité SSL dans notre environnement d'apprentissage virtuel.

ABSTRACT

Currently, the educational establishments cannot be allowed to evaluate the students according to a course via Internet, due to the weak safety of this environment. The establishments wish to obtain the note of the highest credibility than possible and this begins with the manner of evaluating the students. The universities must make safe their learning environments in order to offer distance education. The two principal problems of the current virtual learning environments are: weak safety and impossibility of reaching the environment by mobile equipment.

With the mobile equipment now available on the market to reach Internet, it is essential to give the possibility to the students of using them in order to reach the virtual learning environment, without however forgetting safety. In order to improve quality of education and the training, this form of training must be build on a secure environment by offering a quality of service and by allowing the mobility of the person, the terminal and the services.

Mobility in the virtual training inevitably poses a problem of safety, and by far different from safety in the cabled environments. In this thesis, we study questions related to mobile learning environments including security aspects. As m-learning has its own security problems, we will distinctly treat them in order to understand and proposed an adequate solution. We also study the current virtual learning architectures and we propose a secure architecture for a mobile learning environment like a virtual laboratory. Finally, we will evaluate the performance of our architecture.

We build a secure architecture in a mobile learning environment. In order to test our model, we have simulated users in a network WLAN. The principal idea was to compare the performance of our architecture with a similar architecture without safety.

Simulations carried out in WLAN environment show that the secure mechanisms used are a reasonable price to pay in order to ensure the security in virtual learning environments. Performance evaluation also allowed us to quantify the cost of implementation of the secure mechanism SSL in our virtual learning environment.

TABLE DES MATIÈRES

LISTE DES FIGURES

LISTE DES TABLEAUX

LISTE DES SIGLES ET ABRÉVIATIONS

DMZ	Demilitarized Zone
EAP	Extensible Authentication Protocol
FTP	File Transfert Protocol
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPSec	Internet Protocol Security
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure
MIC	Message Integrity Check
M-learning	Mobile learning
PDA	Personal Digital Assistant
PGP	Pretty Good Privacy
QoS	Quality of Service
RADIUS	Remote Authentication Dial-In User Service
SSL	Secure Socket Layer
VLE	Virtual Learning Environment
VPN	Virtual Private Network
WAP	Wireless Application Protocol
WEP	Wired Equivalent Privacy
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access

CHAPITRE I
INTRODUCTION

Les nouvelles technologies permettent de plus en plus aux usagers d'accomplir leurs tâches où bon leur semble, en particulier grâce à des appareils mobiles qui facilitent le nomadisme. Toutefois, les exigences des utilisateurs face à ces appareils mobiles sont élevées. En effet, les utilisateurs désirent retrouver, sur ces appareils, les mêmes services que ceux offerts sur les ordinateurs maison. Ils désirent aussi avoir accès aux services auxquels ils sont abonnés en toute liberté. La venue de ces appareils mobiles sur le marché a donc ouvert la voie à plusieurs concepts nouveaux dont le *e-learning* (electronic learning) ou *apprentissage électronique*, basé sur Internet, sans présence physique de l'étudiant dans une classe. Ainsi, tant sur les ordinateurs fixes que sur les appareils mobiles (cellulaire, PDA), les utilisateurs pourront suivre leur « e-cours » où bon leur semble et au moment qui leur convient le mieux. Cette forme d'apprentissage se déployant sur Internet pose inévitablement le problème de la sécurité qui fait l'objet de ce mémoire. Dans ce chapitre d'introduction, nous allons présenter quelques définitions et concepts de base, préciser les éléments de la problématique, fixer les objectifs de recherche, et enfin esquisser le plan du mémoire.

1.1 Définitions et concepts de base

L'enseignement a évolué depuis les toutes premières formes d'enseignement à distance. À l'origine, la *formation à distance* consistait à la transmission du savoir entre les différents acteurs (enseignants, étudiants) représentés dans une dispersion géographique. Les formes de communications entre l'étudiant et l'enseignant étaient asynchrones et centrées sur le courrier, qui circulaient sous la forme de documents physiques (en papier). Selon Tapsall et Ryan (1999), la formation à distance vise principalement à résoudre le problème de la distance entre les apprenants et les établissements d'enseignement, en se basant sur le fait que les responsabilités personnelles peuvent empêcher les apprenants de se rendre régulièrement sur le campus

pour assister aux cours. L'évolution de l'enseignement nous amène à considérer non seulement le courrier comme support de communication mais aussi le réseau informatique. D'où est né l'apprentissage électronique ou *e-learning*. L'*apprentissage électronique* désigne généralement l'utilisation de réseaux numériques, synchrones ou asynchrones, pour l'acquisition de connaissances, la diffusion et l'administration des contenus de formation. De manière plus explicite, il intègre les aspects suivants :

- les modalités administratives telles l'inscription, les dossiers, les frais, etc ;
- l'élaboration, la production et la distribution du matériel didactique ;
- les services de soutien aux apprenants, notamment l'orientation professionnelle, les consultations, l'évaluation des connaissances acquises, la planification des programmes et l'accès aux ressources documentaires.

L'enseignement en ligne nous permet d'améliorer la productivité, l'efficacité et la qualité des fonctions de base en utilisant les technologies de l'information et des communications (TIC) appropriées. En particulier, les TIC sont utilisées pour l'administration et l'élaboration de matériel didactique depuis un bon moment, mais leur application à l'organisation et la gestion des contenus ne fait que commencer.

L'évolution récente des moyens de communication sans fil a permis la manipulation de l'information à travers des unités de calcul portables ayant des caractéristiques particulières (faible capacité de stockage, source d'énergie autonome, etc.) et l'accès au réseau à travers une interface de communication sans fil. Comparativement à l'environnement classique statique, le nouvel *environnement mobile* ainsi créé permet aux unités de calcul une libre mobilité et n'impose presqu'aucune restriction sur la localisation des usagers. La mobilité et le nouveau mode de communication utilisé engendrent de nouvelles caractéristiques propres à l'environnement mobile : une fréquente déconnexion, un débit de communication plutôt faible, des ressources modestes et des sources d'énergie limitées. De ce type d'environnement est né l'*apprentissage mobile* ou *m-learning* (mobile electronic learning), la génération précédant le *e-learning* où les technologies sans fil tel que le téléphone cellulaire, le PDA ou l'ordinateur portable sont utilisés pour acquérir des notions de cours.

Le concept de *mobilité* dans l'apprentissage vient du fait que l'usager n'a pas à assister physiquement à un cours à un moment et en un lieu précis. Nous entendons par *apprentissage mobile* un apprentissage structuré et supervisé par l'enseignant, stimulant la collaboration entre les professionnels et les étudiants (par l'accès au «chat», courriel, forum, etc.) afin d'améliorer la qualité de l'éducation et de l'apprentissage; cette forme d'apprentissage doit reposer sur un environnement sécuritaire, peu importe l'utilisation du médium, en offrant une qualité de service satisfaisante et en permettant la mobilité de la personne, du terminal et des services.

Le concept de *campus virtuel* correspond à une démarche visant à reproduire l'environnement (l'institution) virtuellement. D'où est né l'*environnement d'apprentissage virtuel* (VLE : Virtual Learning Environment). Le VLE est essentiellement un site Web qui fournit des fonctionnalités de base estimées essentielles dans le processus d'apprentissage. Normalement, un ensemble d'outils et d'aides de navigation sont fournis ayant pour but d'accéder à tout matériel et aide pédagogique. Un tel environnement fournit aux étudiants un accès facile aux matériels offerts : documents d'apprentissage, aux notes de cours, aux questionnaires, aux outils de support et aux outils de communications.

Les utilisateurs de VLE sont divisés en deux grandes classes : étudiants et professeurs. Les professeurs possèdent des outils additionnels afin de leur permettre d'ajouter et de modifier du matériel, créer des conférences et suivre le progrès des étudiants. Normalement, les étudiants possèdent une section de conférence qui ne peut être vue du professeur. Un système VLE est basé sur une architecture client/serveur. En général, le client est simplement un navigateur qui est utilisé pour accéder aux pages HTML sur le serveur.

Le concept de *laboratoire virtuel* permet l'actualisation du travail collectif en temps réel, l'interactivité dynamique des chercheurs, qui rendent visible le processus de leur travail (hypothèse, expérimentation, discussion, validation, résultats). Ainsi, le laboratoire virtuel a le potentiel de briser des barrières à la fois temporelles et spatiales.

1.2 Éléments de la problématique

La sécurité dans les environnements d'apprentissage est un concept tout récent. C'est pourquoi on y compte très peu ou pas de travaux élaborés sur ce sujet. L'apprentissage mobile n'est sujet à aucune norme de sécurité. En effet, chaque site qui offre l'apprentissage mobile propose ses propres mécanismes de sécurité, quand ils sont présents. Le problème souvent mentionné s'exprime par les questions suivantes : comment peut-on assurer la confidentialité des transactions de *e-learning?* Comment obtenir une marque de confiance du public par l'apprentissage dans un environnement tel qu'Internet? Anderson (2001) réalise l'importance de la sécurité au niveau du *e-learning* dans son court rapport « Secure and credible e-learning systems », mais ne propose aucune architecture afin de résoudre les problèmes identifiés. Selon lui, la plus difficile et cruciale étape afin d'établir la crédibilité du *e-learning* est le développement d'un environnement sécuritaire. En effet, plusieurs modèles sont proposés à partir des problèmes de sécurité auxquels les systèmes d'information font face, sans toutefois être développés. En fait, le *e-learning* partage plusieurs de ces problèmes, mais avant tout possède ses problèmes uniques sur le plan sécurité qui doivent être traités distinctement.

Pour garantir cette sécurité dans le *e-learning*, il faut d'abord répondre à certaines questions : Quels sont les problèmes de sécurité dans un environnement mobile? Est-ce que la sécurité peut affecter la qualité des services du *e-learning*? Comment peut-on implanter une architecture sécuritaire dans un environnement mobile? Comment utiliser les réseaux existants afin de bâtir cet environnement sécuritaire? Comment élaborer une architecture sécurisant autant les appareils mobiles sans fil que les appareils avec fil?

La sécurité dans un milieu d'apprentissage repose essentiellement sur la sécurité des techniques d'évaluation de l'apprentissage. Ces techniques permettent d'assurer la sécurité lors de l'envoi d'un travail à travers Internet, d'assurer la confidentialité de document (travaux de groupe) sur Internet, etc. Celles-ci ont pour but d'assurer la crédibilité des institutions sur Internet. Pour toutes ses raisons, il apparaît indispensable d'élaborer une architecture sécuritaire dans un environnement d'apprentissage virtuel.

1.3 Objectifs de recherche

L'objectif principal de ce mémoire est de concevoir une architecture sécuritaire pour la mise en œuvre d'environnements d'apprentissage mobiles de type laboratoires virtuels permettant aux étudiants de recevoir le même niveau de sécurité, indépendamment des équipements spécifiques d'accès dont ils disposent. De manière plus spécifique, ce mémoire vise à :

- analyser les mécanismes existants de sécurité dans les systèmes répartis eu égard à leur applicabilité au contexte des environnements d'apprentissage mobiles ;
- concevoir de nouveau mécanismes capables de garantir la confidentialité des données et l'authentifications des usagers dans ces environnements ;
- évaluer la performance de cette architecture sous l'angle non seulement de la sécurité mais aussi de la qualité de service qu'elle est capable d'offrir.

1.4 Plan du mémoire

Ce document est organisé comme suit : le premier chapitre, en guise d'introduction, précise, entre autres, la problématique et les objectifs de recherche. Le second chapitre analyse les tendances actuelles en matière de sécurité, les facteurs importants de la sécurité, les coûts se rattachant à la sécurité et la sécurité en contexte de mobilité. Le chapitre trois propose des mécanismes de sécurité et de qualité de service pour les environnements d'apprentissage mobiles de type laboratoire virtuel. Le quatrième chapitre évalue la performance des mécanismes proposés. Finalement, le chapitre de conclusion fait une synthèse des travaux réalisés, en précise les limitations et indique des directions de recherche future.

CHAPITRE II
TENDANCES ACTUELLES DE LA SÉCURITÉ

Les entreprises et les individus dépendent de plus en plus des systèmes informatiques. Ces derniers, connectés en réseau, ont envahi toutes les activités humaines et l'information qu'ils manipulent constitue un enjeu stratégique. Parmi les craintes les plus souvent évoquées par les utilisateurs concernant le commerce électronique figure notamment la problématique de la sécurité. Dans ce contexte, l'authentification des usagers, le contrôle des accès aux machines et aux services, la confidentialité et l'intégrité de l'information, ainsi que la protection des services, deviennent primordiaux. Il faut donc cibler les problèmes de sécurité et apporter une protection aux utilisateurs. C'est dans cette optique que sera développé ce chapitre. Nous y présenterons une définition du concept de sécurité, les facteurs importants de la sécurité, les coûts de la sécurité, la sécurité en contexte de mobilité et finalement les comparaisons entre différents environnements d'apprentissage.

2.1 Définition du concept de sécurité

Lorsqu'on parle de sécurité, on pense souvent à deux idées : protection et tranquillité d'esprit. La sécurité informatique est la somme de toutes les mesures de protection prises pour prévenir les pertes de toutes sortes afin d'assurer la tranquillité d'esprit. La sécurité informatique est un processus continuel et proactif. Le but de la sécurité informatique consiste à maintenir les trois caractéristiques suivantes : *confidentialité, intégrité et accessibilité.*

La confidentialité signifie que les données du système informatique sont accessibles seulement par les parties autorisées. Toutefois, il reste à régler un problème : qui est « autorisé »? L'intégrité signifie, quant à elle, que les données ne peuvent être

modifiées que par les parties autorisés. Dans ce contexte, le terme « modifier » inclut « écrire », « changer », « effacer » et « créer ». Welke et Mayfield (1990) reconnaissent trois aspects de l'intégrité : action autorisée, séparation et protection des ressources, détection d'erreur et correction. L'intégrité peut être renforcée par un contrôle rigoureux de l'identité de la personne, du type de ressources visé et de la manière d'y accéder. Enfin, l'accessibilité signifie que les données sont disponibles uniquement aux parties autorisées. Elle s'applique à la fois aux services et aux données. La sécurité informatique est souvent représentée comme à la Figure 2.1, qui montre comment les trois caractéristiques de la sécurité sont indépendantes mais se chevauchent. Dès que l'une de ces caractéristiques est compromise, le système est propice aux attaques.

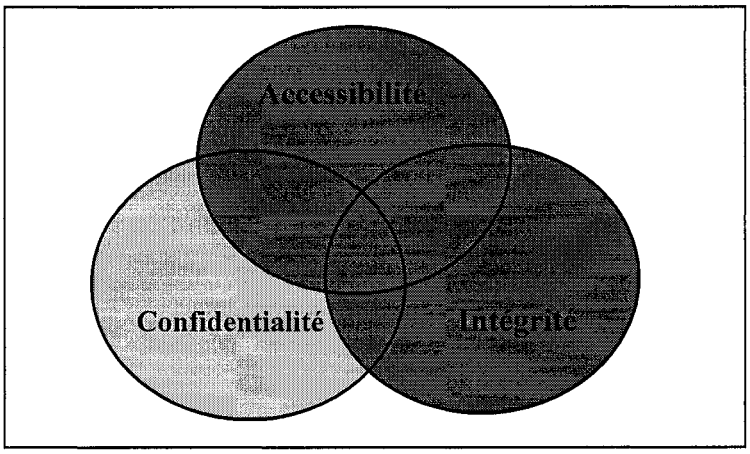

Figure 2.1 Caractéristiques de sécurité

2.2 Attaques potentielles

Les attaques sont construites en se basant sur la négligence d'une des trois caractéristiques de la sécurité. Les différents types d'attaque se retrouvent à l'intérieur de six groupes : attaque basée sur le Web, intrusion interne, déni de service distribué, code malicieux, négligence et fausse authentification de l'usager.

Attaque basée sur le Web

Les attaquants Web, communément appelés « hackers » gagnent l'accès du système et de l'information qu'il contient afin d'exploiter les défauts de configuration du serveur Web et des composantes de la page Web.

Intrusion interne

L'intrusion interne est effectuée par un individu appartenant à l'organisation et pouvant potentiellement avoir un accès autorisé aux composantes logicielles et matérielles. La sécurité physique et les mots de passe sécuritaires permettent de contrôler les activités illégales dans l'organisation.

Deni de service distribué

Le "Distributed Denial of Service" (DDoS) consiste à rendre une ressource inaccessible par saturation ou par destruction. Ainsi, il sature un service par de fausses requêtes afin d'empêcher les vraies demandes d'être servies. "Smurf" et "Syn Flood" sont deux techniques d'attaques de déni de service distribué. L'une comme l'autre consiste à inonder le serveur de demandes de connexions permettant d'accéder à un site Internet. La technique du "Syn Flood" envoie les demandes assorties d'une fausse adresse d'origine, ce que les experts appellent le "spoofing". Cela augmente la confusion du serveur, suivi de son engorgement voire de son arrêt. Ce type d'attaque est efficace car l'Internet est constitué d'un nombre limité et consommable de ressources.

Code malicieux

Contrairement à un virus qui requiert un utilisateur pour l'activer afin de le propager, le code malicieux peut se propager par lui-même. Un code malicieux est un code conçu pour corrompre les données des utilisateurs, permettre des accès illicites à des données ou à des ressources critiques, provoquer un déni de service ou effectuer toute autre action nuisible sans la connaissance et le consentement de l'utilisateur.

Négligence

La négligence face à des données critiques ou à la configuration d'un système de sécurité peut être dévastatrice. Le meilleur système de sécurité incorrectement administré augmente les risques potentiels d'attaques. Des procédures d'administration inadéquates peuvent résulter des failles de sécurité et ainsi ouvrir la porte à des attaques.

Authentification de l'usager

La création et la gestion adéquate d'un mot de passe, la technique de biométrie ou autre mesure d'authentification sont des processus qui requièrent du temps et de l'attention afin de maximiser la sécurité. Certaines attaques utilisent de fausses authentifications afin d'accéder au système.

2.3 Les facteurs importants de la sécurité

Un système fortement sécurisé base sa structure sur plusieurs services sécurisés. Les caractéristiques de sécurité décrites en début de chapitre se réfèrent à la sécurité au niveau du réseau, alors que le concept de *e-learning* apporte de nouveaux critères de sécurité qui s'ajoutent à ceux de réseau. Dans cette section, nous décrirons les concepts de sécurité en rapport avec le *e-learning*, soit l'intégrité et la confidentialité, l'accessibilité, l'authentification, la non répudiation ainsi que les méthodes actuelles pour faire respecter ces concepts.

2.3.1 Confidentialité et intégrité

La confidentialité et l'intégrité consistent à assurer que les données reçues soient bien celles envoyées et qu'elles n'aient pas été interceptées. La confidentialité des données vise comme objectif d'assurer que les messages transmis ne peuvent être lus que par l'émetteur et le destinataire. L'intégrité consiste à s'assurer que le message n'a pas été modifié pendant sa transmission et que le message qui arrive au destinataire est bien celui qui a été envoyé par l'émetteur. Pour ces deux services de sécurité, deux approches existent. La première consiste à utiliser un canal sécurisé afin d'envoyer en

clair les données sur le canal. Ainsi, on fait confiance à une infrastructure de transport afin d'acheminer le message. C'est le cas pour les Virtual Private Networks (VPN) ou les sessions SSL (HTTPS). La seconde consiste à utiliser un canal non sécurisé et à faire reposer la sécurité sur les messages eux-mêmes. Cette approche offre une grande souplesse, car elle permet d'utiliser tout canal de communication, en particulier Internet.

Les trois principales technologies utilisées par les canaux sécurisés sont les suivantes :

- IPSec (Internet Protocol Security): Il s'agit d'un protocole développé par l'IETF fournissant un mécanisme de sécurisation au niveau de la couche réseau. Il offre l'authentification des échanges entre deux équipements, la confidentialité et l'intégrité des données échangées. L'avantage de ce protocole est de permettre une sécurisation de toute communication passant sur IP et indépendante des protocoles (HTTP, FTP...). On retrouve IPSec dans IPv6, mais il ne peut être implanté dans IPv4 qui est utilisé aujourd'hui.
- SSL et TLS (Secure Socket Layer / Transport Layer Security) est un protocole (développé par Netscape et repris par IETF sous le nom de TLS) fournissant un mécanisme de sécurisation au niveau transport de l'application. L'utilisation conjointe de SSL et de HTTP résulte du protocole HTTPS. L'utilisation de SSL authentifie un serveur et permet d'authentifier le client par l'utilisation de certificat. SSL permet ensuite le chiffrement de la liaison établie à l'aide d'algorithmes asymétriques qui consiste à utiliser des clé différente pour le chiffrement et le déchiffrement.
- VPN (Virtual Private Networks) est un service disponible chez les fournisseurs de services Internet qui permet d'établir des connexions sécurisées privées (un réseau privé) sur un réseau public comme l'Internet. Le VPN est réalisé avec les techniques d'encryption et d'authentification, en assurant la qualité de services requise. Le VPN permet l'économie de connexions directes coûteuses entre les différentes implantations de l'entreprise, l'accès Internet lui servant à la fois pour la consultation classique de sites Web et pour son réseau privé. La Figure 2.2 illustre un VPN.

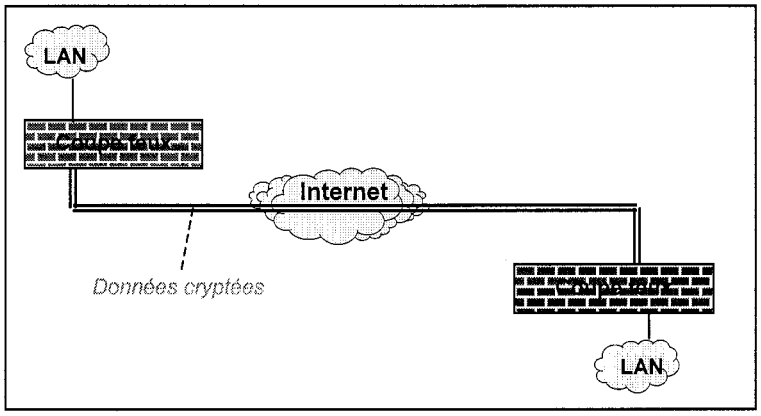

Figure 2.2 Exemple de VPN

Les technologies utilisées afin de sécuriser les messages envoyés sont :

- S/MIME : S/MIME est la version sécurisée du protocole MIME utilisé pour le courrier électronique. Il propose l'authentification et le chiffrement des données à travers l'utilisation de certificat personnel. Son utilisation est faite de manière transparente pour l'utilisateur à travers son logiciel client « mail » en cliquant sur des boutons chiffrer et signer.
- PGP (Pretty Good Privacy) : est un logiciel de signature et de chiffrement gratuit. L'objectif est de proposer au plus grand nombre d'individus des outils permettant d'assurer une certaine confidentialité sur Internet. Il repose sur l'utilisation de certificats possédant un format spécifique PGS, et sur l'utilisation d'annuaires où les certificats des autres utilisateurs peuvent être trouvés. Tout comme S/MIME, PGP permet de chiffrer et d'authentifier les courriers électroniques par simple clique.

2.3.2 Accessibilité

Kagal et al. (2001) indiquent que les petits réseaux s'appuient sur l'authentification des usagers et l'accessibilité afin d'établir la sécurité. L'accessibilité physique aux ressources du système d'information est la première barrière à mettre en œuvre dans la conception d'une architecture de sécurité. Inutile de déployer des systèmes de sécurité complexes si l'accès au serveur n'est pas contrôlé. Le contrôle d'accès consiste à

appliquer des filtres dans le monde réel (clé, carte magnétique,...) et des filtres dans le monde virtuel afin de garantir que seuls les flux autorisés transitent. Les filtres appliqués dans le monde virtuel peuvent être un filtrage protocolaire qui consiste à surveiller les ports de communication et gérer l'ouverture des ports selon le protocole. Afin d'implémenter un filtrage protocolaire, on utilisera une architecture coupe-feu, un système de détection d'intrusion ou des réseaux privés virtuels.

L'architecture coupe-feu assurera le contrôle d'accès aux applications, l'isolement du réseau extérieur, l'authentification des utilisateurs, ainsi que le chiffrage des échanges. Ce type d'architecture de sécurité introduit les notions de zone militarisée et zone démilitarisée (MZ et DMZ). Les zones sont séparées chacune par des systèmes de coupe-feu. La zone DMZ, comme illustrée à la Figure 2.3, contient les logiciels serveurs qui communiquent avec l'autre zone de niveau de confiance différent. Il est important de noter qu'aucune donnée critique n'est placée dans cette zone.

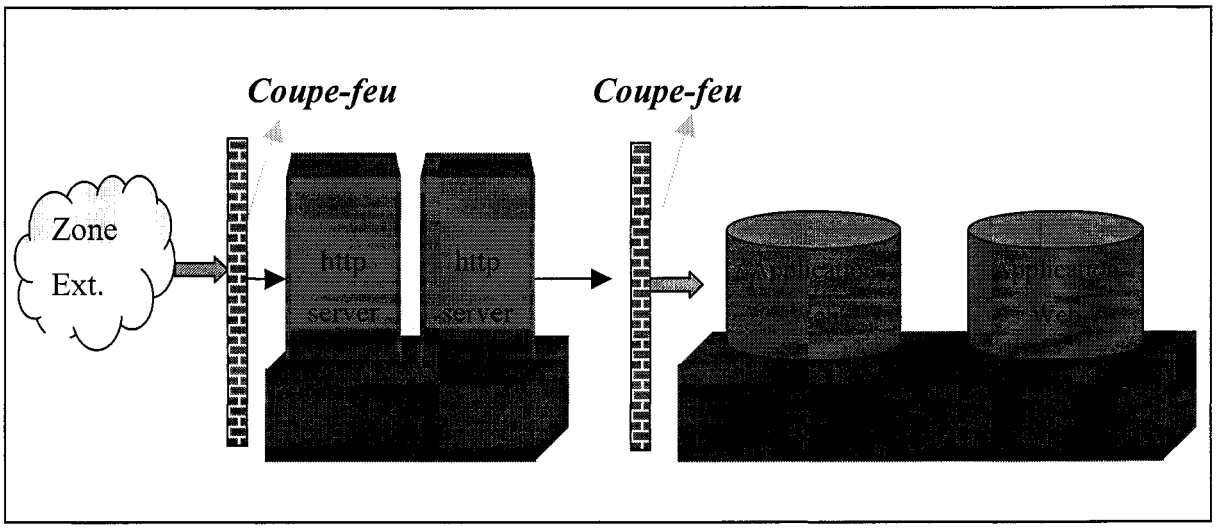

Figure 2.3 Architecture coupe-feu

Le système de détection d'intrusion analyse le trafic réseau interne et signale toute anomalie en temps réel. Il peut parfois être confondu avec le coupe-feu. La principale différence entre ces deux méthodes de contrôle d'accès est que le coupe-feu prévient les

intrusions alors que le système de détection d'intrusion réagit seulement s'il soupçonne une intrusion.

Les réseaux privés virtuels (VPN), comme expliqué précédemment, permettent la transmission sécuritaire des communications confidentielles sur Internet. Ils procurent un accès sécurisé aux données du réseau local, tout en permettant une mobilité aux utilisateurs. L'utilisateur peut ainsi accéder de façon sécuritaire au réseau interne de l'entreprise au moyen d'un réseau privé virtuel.

L'idée générale du contrôle d'accès est de centraliser un maximum de fonctionnalités en un point unique et de contrôler l'accès à ce passage dans les différentes zones du système.

2.3.3 Authentification

Le système d'authentification est fréquemment utilisé pour restreindre l'accès au contenu spécifique. L'authentification regroupe deux fonctions distinctes et complémentaires : l'identification et l'authentification. L'identification consiste à associer une entité numérique à une personne se connectant à un système. Souvent cette fonction est remplie par l'utilisation d'un « login ». L'authentification, pour sa part, vérifie et confirme que la personne qui s'est identifié est bien celle qu'elle prétend être. Cette fonction est souvent remplie par l'utilisation d'un mot de passe. Le service d'authentification constitue la base d'une sécurité orientée vers utilisateur. C'est de ce service que découle l'ensemble des services de sécurité dans un environnement Internet, quels que soient les échanges que l'on désire rendre sécuritaires (utilisateur versus utilisateur, utilisateur versus serveur ou serveur versus serveur).

Au début des années 90, l'utilisation du Web était purement consultative, les entreprises cherchaient juste à avoir une présence sur la toile avec un simple site informatif, l'authentification de l'utilisateur était alors fondée sur l'utilisation d'un simple mot de passe afin de gérer le droit d'accès sur le contenu. Aujourd'hui, avec la venue du commerce électronique, les entreprises proposent des services de haut niveau

centré sur l'utilisateur (paiement en ligne,...) et manipulent des données plus sensibles (carte de crédit). Il est donc impératif d'avoir une authentification sûre de l'utilisateur.

2.3.3.1 Méthodes d'authentification

Les méthodes d'authentification reposent sur l'utilisation d'un secret. Les progrès de la technique (mathématique, cryptographie, électronique, miniaturisation, reconnaissance des formes,...) ont permis de répondre aux besoins actuels d'authentification pour lesquels la seule utilisation du mot de passe n'était plus suffisante. Selon le genre de secret, trois types d'authentification peuvent être distingués :

- *Authentification par « ce que je sais »* : le secret repose ici sur une donnée connue par l'entité qui désire s'authentifier. Le secret correspond au mot de passe. Le mécanisme de « storage » repose sur la mémoire propre de l'individu , celle-ci étant la forme de « storage » la moins chère et la plus facile à gérer. Par contre, cette forme d'emmagasinage des données n'est pas sécuritaire. Une difficulté importante à l'utilisation de mots de passe est la transmission de celui-ci de manière sécurisée afin d'éviter le vol du mot de passe. L'avantage est qu'aucun support de lecture n'est nécessaire.
- *Authentification par « ce que je possède »* : le secret repose ici sur la possession physique d'un objet et d'un secret par l'entité désirant s'authentifier. Cela peut être une clé, une carte ou tout autre support. L'avantage d'un tel système repose sur la difficulté à reproduire l'objet. Par contre, un support de lecture est obligatoire afin d'effectuer la lecture de l'objet.
- *Authentification par « ce que je suis »* : le secret repose ici sur l'individu même ou plutôt une partie de l'individu. Ce type d'authentification fait généralement référence à la biométrie et donc à l'authentification de personnes physiques. Ce type d'authentification assure la présence de l'individu, mais là encore un support de lecture est obligatoire.

2.3.3.2 Techniques d'authentification

Il existe plusieurs techniques d'authentification autres que le simple mot de passe que nous verrons dans cette section telles que le certificat, le support physique d'authentification et la biométrie.

Certificat

Un certificat est un fichier qui contient des informations sur son propriétaire (nom, prénom, adresse électronique, ...) ainsi que la clé publique de celui-ci. Il est signé par une autorité, ce qui garantit la validité des informations contenues dans ce fichier. Un certificat est associé à la clé privée de son propriétaire, qui n'est pas contenue dans ce certificat mais généralement enregistrée sur le poste de travail de l'utilisateur. Avec ce certificat et sa clé privée, l'utilisateur peut signer son courrier électronique et accéder à des pages à accès contrôlé.

La première méthode de distribution de certificat est d'avoir une relation de confiance directe avec son détenteur, comme dans le modèle "Web of trust" associé à PGP. La deuxième façon est que tous les interlocuteurs aient confiance en un tiers, qui certifiera les clés en les signant. Il appartient aux émetteurs de certificats, ou autorités de certification, de s'assurer que telle clé appartient bien à telle personne (ou entité), et de publier les procédures définissant cette assurance (politiques de certification).

Un certificat contient les données suivantes : Version du certificat, numéro de série du certificat, description de l'algorithme de signature de l'AC (autorité de certification), nom de l'AC qui a généré le certificat, période de validité, nom de l'utilisateur auquel appartient le certificat, valeur de la clé publique, description de l'algorithme à utiliser avec la clé publique et la signature de l'AC. Le certificat est fiable mais il reste associé à une machine, ce qui en réduit la mobilité.

Support physique d'authentification

L'utilisation d'un support physique consiste à utiliser un objet pour effectuer l'authentification. Aujourd'hui, il existe deux principaux types de support : la clé USB et la carte à puce (ex : SecureID, SmartCard).

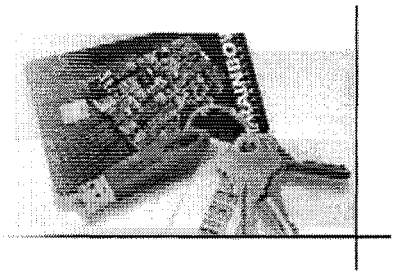

Figure 2.4 Clé Usb (Ikey)

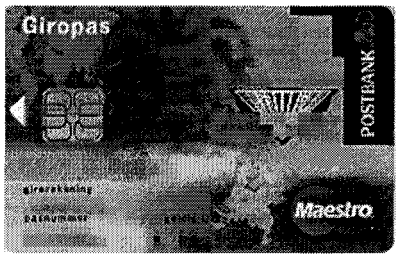

Figure 2.5 SmartCard

L'utilisation de ce type de support présente plusieurs avantages dont la possession d'un objet par rapport à l'utilisation de mots de passe. Contrairement au mot de passe, l'utilisateur est conscient lorsque le support est volé. De plus, le support peut contenir des informations de type certificat numérique qui permettent le cryptage des échanges en plus de l'authentification.

Par contre, l'utilisation de ce type de support nécessite la mise en place d'une infrastructure pour la création et la gestion des supports. Les données personnelles d'authentification doivent être inscrites sur le support. Cette opération peut être réalisée par un opérateur ou par l'entreprise. Le second inconvénient est la nécessité de posséder un support de lecture de carte. Les clés USB, quant à elles, présentent l'avantage de se brancher directement sur le port USB de l'ordinateur. La Figure 2.6 présente différents lecteurs de carte.

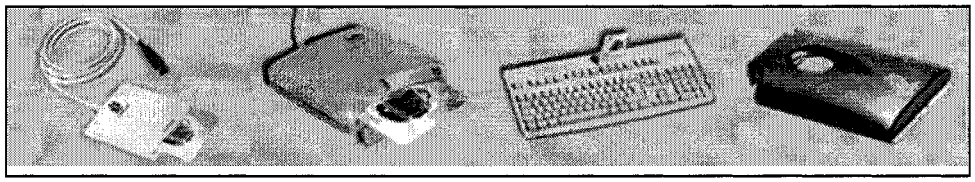

Figure 2.6 Lecteurs de carte à puce

Biométrie

La biométrie est une technique globale visant à établir l'identité d'une personne en mesurant une de ses caractéristiques physiques et non plus par un élément externe qui peut être dérobé. Ainsi, lors de l'authentification, la présence de l'individu devient nécessaire. Actuellement, le test d'identification par biométrie peut s'effectuer aussi bien à partir d'une empreinte digitale qu'à partir de la voix, du visage entier, de l'iris, d'une empreinte rétinienne, d'analyse des mouvements de la personne (style d'écriture, la démarche, la vitesse de frappe sur un clavier etc.) Il peut y avoir plusieurs types de caractéristiques physiques, les unes plus fiables que d'autres, mais toutes doivent être infalsifiables et uniques pour pouvoir être représentatives d'un et d'un seul individu.

Le principal avantage de la biométrie est son haut niveau de sécurité dû à la nécessité de la présence de l'individu durant l'authentification. Par contre, il existe plusieurs freins au développement de la biométrie tels que :

- L'évolution de ce qu'on mesure : le corps humain vieillit, ce qui signifie qu'avec le temps il y a divergence entre l'empreinte enregistrée et la mesure faite sur le corps ;
- L'altération possible de ce que l'on mesure : les mesures biométriques vont être sensibles aux différents accidents qui peuvent intervenir dans la vie de l'individu qui s'authentifie ;
- Le coût actuel élevé : les appareils pour faire la reconnaissance sont actuellement très chers ;
- Le vol du secret : il existe toujours la possibilité de se faire voler l'objet de la reconnaissance (ex : se faire couper un doigt) et ce type de vol est plus coûteux qu'un mot de passe ;

- La mauvaise authentification : La biométrie utilise des techniques de reconnaissance de forme où le taux d'erreur est présent. Il est donc possible de ne pas authentifier la bonne personne ;
- Le manque de standard : Aujourd'hui, il n'existe pas de standards de la biométrie.

Il est possible de mesurer plusieurs caractéristiques uniques pour un individu dont les plus populaires sont : l'empreinte digitale, l'iris-scan, le visage scan et la signature scan.

Empreinte digitale : La donnée de base dans le cas des empreintes digitales est le dessin représenté par les crêtes et sillons de l'épiderme. Ce dessin est unique et différent pour chaque individu.

Figure 2.7 Empreinte digitale

Les diverses techniques utilisées pour la mesure sont les capteurs optiques, ultrasoniques, de champ électrique, de capacité et de température. Ces capteurs sont souvent doublés d'une mesure visant à établir la validité de l'échantillon soumis, c'est-à-dire de vérifier qu'il s'agit bien d'un doigt. Cette dernière mesure la constante diélectrique relative de l'échantillon, sa conductivité, les battements de coeur ou la pression sanguine.

Iris-scan : L'individu se place en face du capteur qui scanne son iris. Celui-ci représente quelque chose de très intéressant pour la biométrie car l'iris est à la fois toujours différent, même entre jumeaux et également entre l'oeil gauche et le droit d'un même individu. Ce type d'authentification est indépendant du code génétique de l'individu, et très difficilement falsifiable.

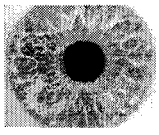

Figure 2.8 Iris

Visage scan : Il s'agit ici de faire une photographie plus ou moins évoluée pour en extraire un ensemble de facteurs qui se veulent propres à chaque individu. Ces facteurs sont choisis pour leur forte invariabilité et concernent des zones du visage telles que le haut des joues, les coins de la bouche, etc. On évitera d'autre part les types de coiffures, les zones occupées par des cheveux en général ou toute zone sujette à modification durant la vie de la personne. Il existe plusieurs variantes de la technologie de reconnaissance du visage. La première est développée et supportée par le MIT et se nomme "Eigenface". Elle consiste à décomposer le visage en plusieurs images faites de nuances de gris, chacune mettant en évidence une caractéristique particulière, comme le démontre la Figure 2.9.

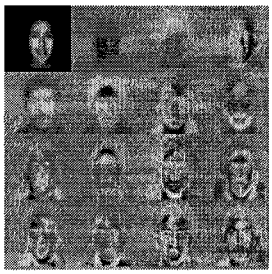

Figure 2.9 Visage scan

Une autre technique appelée "feature analysis" se base sur la précédente en y rajoutant des informations sur les distances inter-éléments, leurs positions, etc. Elle se dit plus souple quant aux éventuelles modifications pouvant survenir : angle de prise de vue, inclinaison de la tête, etc.

Signature scan : Ce type de biométrie est actuellement peu utilisé mais sera pratique pour des applications spécifiques (documents électroniques, rapports, contrats...). Le procédé est habituellement combiné à une palette graphique munie d'un stylo. Ce dispositif va mesurer plusieurs caractéristiques lors de la signature, telles que la vitesse, la pression et les accélérations, le temps total, etc. Bref, tout ce qui peut permettre d'identifier une personne de la façon la plus sûre possible quand on utilise une donnée aussi changeante que la signature.

Le résultat d'une étude effectuée par la compagnie « International Biometric Group » illustré à la Figure 2.10, présente les différents critères pour chaque type de technique biométrique.

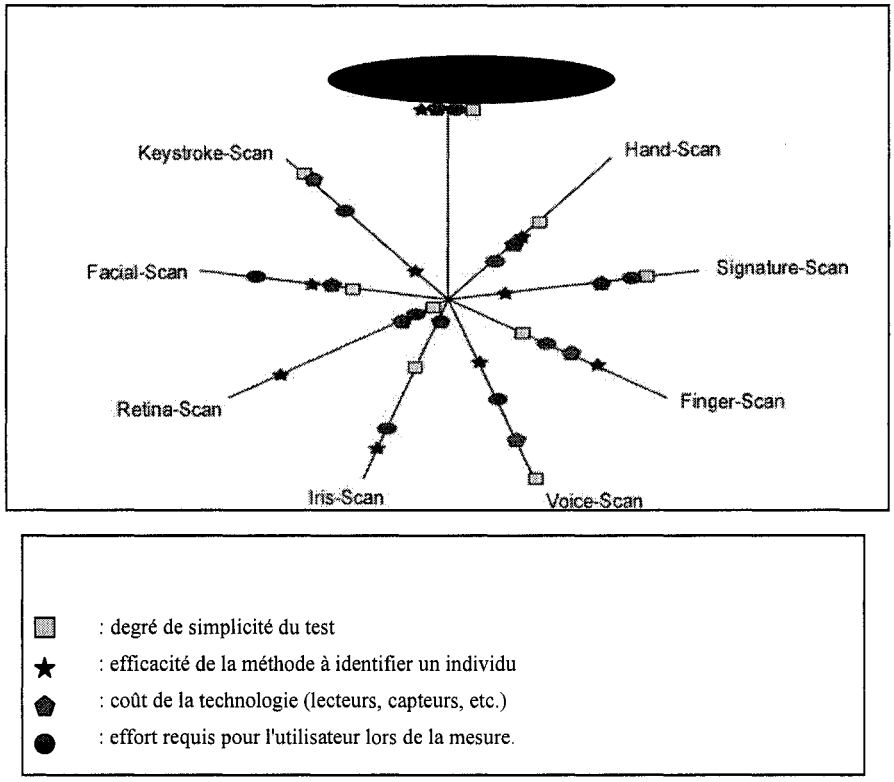

Figure 2.10 Analyse des techniques de biométrie

En se référant à la Figure 2.10 nous constatons que le facial scan est moyennement coûteux et reste une méthode efficace pour identifier un individu.

2.3.4 Non répudiation

La non répudiation consiste, lors d'un échange, à assurer le destinataire d'un message que l'émetteur est bien celui qu'il dit être, et à l'émetteur que le destinataire a bien reçu le message. Personne ne veut que l'autre partie engagée dans une transaction puisse désavouer ses actions ou nier qu'un échange a eu lieu. C'est dans cette optique que la non répudiation est utilisée. Elle permet de rendre deux services : celui d'authentifier l'émetteur du message et celui de garantir l'intégrité du message.

Pour une transaction physique, on utilise des reçus, des signatures et des témoins pour confirmer l'engagement. Dans le cas d'une transaction électronique, il faut également qu'un document lie l'émetteur et le récepteur. Les certificats et les signatures sont utilisés pour assurer la non répudiation des transactions.

Tel que présenté dans la section précédente, le certificat est un document sous forme électronique permettant d'assurer la confidentialité, l'authentification et l'intégrité. Le certificat est délivré par une autorité de certification qui atteste la véracité des informations contenues dans le certificat, dont l'identité de la personne. Il assure les principes de non répudiation dans la mesure où le certificat électronique est délivré en suivant une procédure stricte de contrôle et de vérification de l'identité de la personne. Il permet d'authentifier avec certitude l'émetteur d'un message reçu, en plus de garantir l'intégrité de ce message. Ainsi, ayant la signature de l'émetteur, le récepteur est certain que le message n'a pas été modifié ou altéré lors de son passage sur Internet.

La méthode de signature électronique repose sur des procédés fiables basés notamment sur des méthodes de cryptologie fortes, assez complexes, et faisant appel au certificat électronique. Apposée à un document électronique, la signature électronique permet de lier le document à la clef privée de l'auteur du document et de garantir l'intégrité des données. Comme le montre la Figure 2.11, le récepteur peut vérifier que l'émetteur a signé le message, puisque sa clé publique est la seule à permettre le décodage.

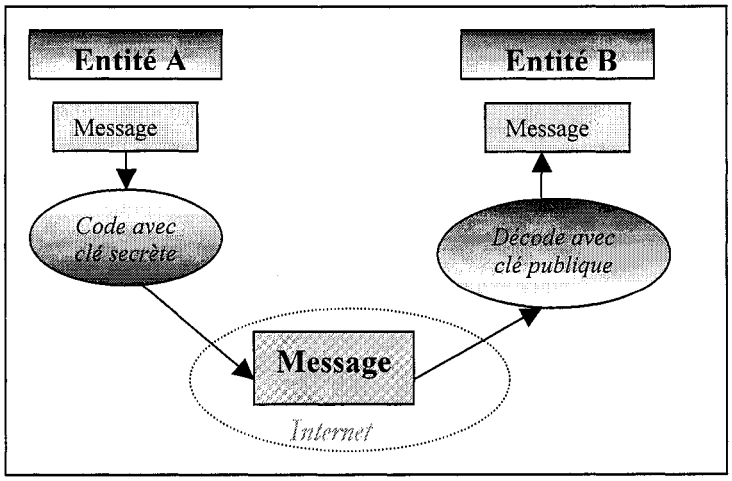

Figure 2.11 Signature électronique

2.4 Les coûts et performance de la sécurité

Ne rien protéger ne coûte rien. Se protéger de tout est impossible et exigerait un coût extrêmement élevé. Il faut évaluer le risque d'un incident, c'est-à-dire les coûts tangibles des ressources utilisées pour revenir à un état normal, par exemple reconstruire un fichier, ainsi que les coûts intangibles, par exemple la perte de clientèle. Le coût d'une protection à 99 % (100 % est impossible) dépasserait probablement le coût des éléments à protéger.

Il est également important de définir les solutions à adopter en fonction:

- des éléments à protéger et contre qui,
- de la valeur de ces éléments ou de leur reconstruction,
- de la probabilité d'occurrence,
- de la perte potentielle,
- des coûts de protection ou de non protection associés.

La Figure 2.12 montre la zone d'équilibre pour un niveau de sécurité acceptable. Le coût du retour à une situation opérationnelle correspond au coût de remise en place des services après une attaque.

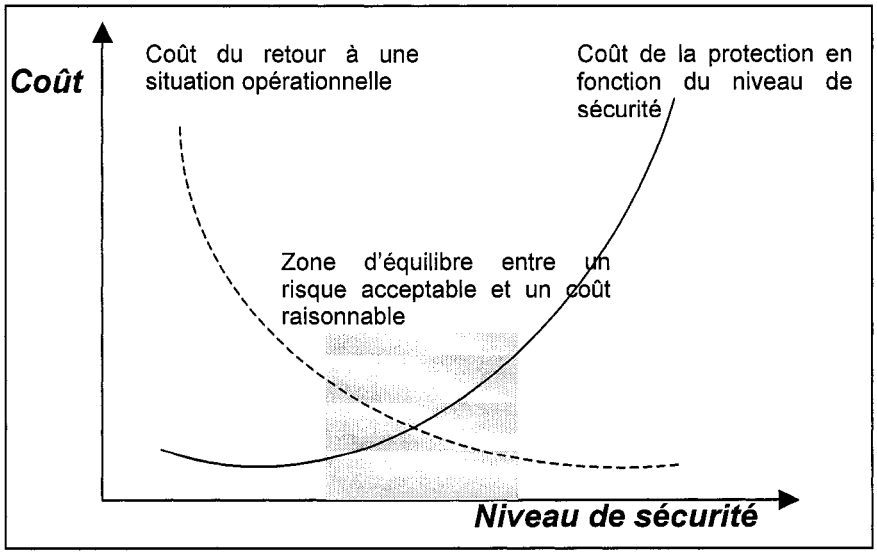

Figure 2.12 Zone d'équilibre de sécurité

La sécurité reste toujours un compromis entre la valeur protégée et le coût de sa protection.

La performance d'un système est caractérisée par le délai d'accessibilité, le délai de transmission et d'affichage. En y ajoutant des mécanismes de sécurité nous affectons la performance de ce système à différents niveaux. Il faut alors trouver un équilibre entre la performance et la sécurité. En partageant la sécurité à différents niveaux (modèle OSI), la performance du système en est moins affectée et du même coup la sécurité est plus forte. En effet, chaque couche étant munie d'un mécanisme de sécurité, cela assure une plus grande sécurité d'ensemble.

2.5 Sécurité dans les réseaux mobiles

Il y a quelques années à peine, une personne possédant un ordinateur à la maison était considérée comme riche. Aujourd'hui, les élèves apprennent à travailler sur un ordinateur et doivent s'en servir pour remettre leurs travaux. Les adultes autant que les adolescents possèdent leur propre téléphone cellulaire. L'informatique a complètement modifié notre mode de vie, mais aussi transformé complètement nos appareils électroniques. L'évolution des technologies a réduit considérablement la taille de nos appareils, et surtout nous a permis de nous déplacer sans être encombré par les fils. Nous voilà maintenant à l'ère où la majorité possède un appareil mobile afin de communiquer (par Internet, par fax, par appel...) et d'être rejoint en tout temps. La venue de ces nouveaux appareils et leur principe de fonctionnement nous conduit à instaurer des nouveaux mécanismes de sécurité. La sécurité des communications sans fil peut être compromise beaucoup plus facilement que celle avec fil, spécialement si la transmission est sur une large région, indique Forman (1994). Pour l'instant, les connexions sans fil nous apportent une grande mobilité mais au détriment de la sécurité.

Malgré les mécanismes de sécurité déployés dans les réseaux sans fil, la sécurisation de ces derniers constitue un problème critique. Cette insécurité est due en partie aux faiblesses décelées dans les mécanismes de sécurité mais principalement celui du

protocole de sécurité WEP (Wired Equivalent Privacy). Effectivement, WEP présente plusieurs failles dont voici les principales :

- ✓ Faible chiffrement (ex : 40 bits) ;
- ✓ Absence du contrôle d'intégrité par un MIC (message Integrity Check) ;
- ✓ Mauvaise implémentation de l'algorithme RC4 ;
- ✓ Mauvaise gestion des clés ;
- ✓ Utilisation de clé statique.

Pour pallier ces insuffisances, plusieurs solutions sont proposées. Notons entre autres IEEE 802.11i, un protocole de cryptage et de gestion de clés; IEEE 802.1x qui permet la sécurisation de divers médias par le biais de mécanismes d'authentification forte et de serveur RADIUS. Notons aussi le WPA (Wi-Fi Protected Access), qui permet un meilleur cryptage de données en utilisant des clés TKIP (Temporal Key Integrity Protocol). Cela signifie qu'avec le WPA, la clé de chiffrement est dite clé dynamique, c'est-à-dire que la clé change fréquemment dans le temps. Nous ne considérons pas WEP2 qui est la nouvelle version de WEP, car il possède encore des failles. Nous pouvons également utiliser SSL pour sécuriser les applications Web.

2.5.1 Mobilité

La mobilité désigne un déplacement instantané de la personne, du terminal ou des services. Analysons maintenant les différents types de mobilité.

Mobilité de la personne : La mobilité de la personne permet à un utilisateur de se servir de n'importe quel terminal mobile ou fixe disponible à partir de n'importe quel réseau, pour accéder à ses services personnels. La mobilité personnelle est liée à la gestion de la localisation de l'utilisateur et aussi à la gestion de la mobilité des services. Selon Ciancetta (1999), la troisième génération des réseaux mobiles (3G) s'oriente vers la définition d'un identificateur d'utilisateur qui peut être utilisé sur les terminaux mobiles ou fixes afin de permettre la convergence fixe et mobile des services. Le concept VHE

(Virtual Home Environment), que décrit Pujolle (2000), est introduit par la génération 3G pour supporter la gestion de la portabilité des services définis par la mobilité personnelle.

Le concept de mobilité de la personne entraîne des complications dans la sécurité, principalement au niveau de l'authentification de la personne et de la confidentialité. Lorsque l'usager se déplace d'un réseau à un autre, ce dernier doit être en mesure de correctement l'identifier. De plus, il faut assurer une parfaite confidentialité des données appartenant à chaque personne qui visite les stations de travail.

Mobilité du terminal : Lorsqu'on parle de mobilité, on sous-entend habituellement la mobilité des terminaux. On parlera d'un téléphone mobile, d'un ordinateur portable (mobile). La demande de mobilité par le monde des réseaux de données vient de plusieurs facteurs, dont la miniaturisation du matériel (ordinateur portable, PDA). Les utilisateurs exigent de ces équipements les mêmes performances que leur PC à la maison, la promesse de « l'anywhere, anytime » face à l'accès réseau.

La mobilité d'un terminal permet à un terminal mobile de changer son point d'attachement au réseau sans perdre la connexion en cours (Pierre, 2003). Il faut donc trouver un moyen de rester accessible à la même adresse, tout en voyageant dans différents réseaux. Il faut s'assurer que :

- la connexion soit continue, en assurant une transparence vis à vis de l'errance ;
- l'opération soit simple à mettre en œuvre et d'un coût raisonnable ;
- l'accès aux ressources soit transparent.

La principale difficulté au niveau sécurité qui est introduit par le concept de la mobilité de la personne est l'authentification de l'équipement sur un nouveau réseau. En effet, lorsque l'appareil entre dans un nouveau réseau, ce dernier doit être capable d'identifier l'appareil et d'avoir accès aux fonctions propres à son type d'utilisateur.

Mobilité des services : La mobilité des services réfère à la possibilité, pour un usager mobile donné, de pouvoir conserver, modifier et personnaliser ses services tout en étant en mouvement (Bah et al., 2002). En effet, ce type de mobilité permet aux usagers de se déplacer entre les nœuds d'un réseau (mobile ou fixe) tout en étant capable d'accéder à leurs services de façon transparente. Ainsi, le service est indépendant du terminal.

Le concept de mobilité des services est souvent offert par l'intermédiaire des agents mobiles, s'accaparant ainsi des problèmes de sécurité des agents mobiles. Les menaces des agents mobiles sont les différentes attaques qui leur sont lancées. Allée (2001) identifie sept types d'attaque dont la mascarade, le déni de service, l'accès non autorisé (vol d'information), les dégâts, le harcèlement, l'ingénierie sociale et la bombe logique.

2.5.2 Limite de la mobilité

Xu (2001) et Forman (1994) indiquent que la mobilité des appareils présente de nouveaux problèmes tels que :

1) l'authentification assurant que le service n'est pas obtenu frauduleusement ;
2) l'information confidentielle concernant la localisation de l'utilisateur. Par exemple, nous ne désirons pas qu'un cambrioleur soit capable de déterminer quand les habitants d'une maison sont à l'extérieur.

De plus, Maamar (2001) constate que les appareils sans fil souffrent de sérieuses limites relatives à leur capacité de mémoire ainsi qu'à la durée de vie des batteries. Leur mémoire étant plus petite que celle d'un ordinateur, il est donc impossible d'installer tous les protocoles.

La mobilité se heurte bien évidemment à des limités reliées à la sécurité. Certains mécanismes de sécurité sont adéquats pour les terminaux fixes mais ne peuvent être installés sur les terminaux mobiles en raison de la capacité de mémoire des appareils mobiles. De même, en obligeant l'installation de logiciel client de sécurité sur un appareil mobile, nous réduisons la mobilité de l'usager. Ainsi, la sécurité pour les appareils mobiles ne doit pas entraver l'un ou l'autre des types de mobilité.

2.6 Les environnements d'apprentissage actuel

Il y a présentement plusieurs applications qui prétendent être un environnement d'apprentissage virtuel (VLE). L'apprentissage dans un environnement virtuel (VLE) actuellement disponible provient de deux sources différentes, soit commerciale ou institutionnelle. Selon Robert (2002), la première source offre l'apprentissage en ligne tel que *WebCT*, *TopClass*, *LearningSpace* et *Web Course in a Box*, alors que la seconde a pour but d'offrir l'apprentissage en ligne tant sur le campus qu'à l'extérieur. C'est le cas pour *CoMento*, *Learning Landscapes* et *Cose*. Nous avons choisi de vérifier et comparer la sécurité de quelques-uns de ces environnements. Le Tableau 2.1 dresse la liste des applications étudiées ainsi que leur catégorie.

Tableau 2.1 Environnements d'apprentissage virtuel (VLE)

Environnement d'apprentissage	Catégorie
WebCT 4.1	Traditionnel VLE
Blackboard 6	Centre d'apprentissage
Cose 2.05	Collaboration
VLab	Laboratoire virtuel

WebCT 4.1

WebCT (Web Course Tools) fournit un simple environnement pour transmettre le matériel d'apprentissage et gérer l'apprentissage des étudiants. Il fournit toutes ces options à partir de son interface Web afin de faciliter la gestion pour les administrateurs, les professeurs et les étudiants. La sécurité de *WebCT* est supportée par le protocole Secure Socket Layer (SSL) permettant une confidentialité lors des requêtes d'authentification des zones suivantes : nom et mot de passe de l'utilisateur, changement de mot de passe via *myWebCT* et interface administrateur. Aussi, plusieurs options provenant de la sécurité du serveur permettent de prévenir les accès non autorisés et la modification des données. Les autorisations sont allouées par un outil d'autorisation qui assigne l'accès et les privilèges à des utilisateurs spécifiques ou à un

groupe d'utilisateurs. Ainsi, à chaque utilisateur est assigné un rôle d'étudiant, d'enseignant assistant, d'enseignant ou d'administrateur ayant un accès approprié aux outils, fonctions et informations. De plus, *WebCT* supporte l'intégration d'un troisième parti pour l'authentification tel que Kerberos.

WebCT représente un environnement d'exercices, un support à l'apprentissage pour un cours donné physiquement dans un établissement. L'étudiant ne peut y suivre virtuellement un cours dans sa globalité. De plus, *WebCT* posséde les outils de communications tel que le «chat», le forum mais ne possède l'audio-conférence ou la vidéo-conférence.

Blackboard 6

Blackboard Learning System, anciennement *CourseInfo*, permet aux établissements d'enseignement ainsi qu'aux entreprises d'offrir des services administratifs, de communauté ou autres services éducatifs en ligne. Cette plate-forme est disponible en plusieurs versions pour effectuer la distribution de cours, la gestion de communauté et la possibilité d'intégrer des outils API.

Les outils de communication intégrés sont le courriel, le «chat», le forum et le «whiteboard». Cependant, cette plate-forme n'offre pas l'audio-conférence et la vidéo-conférence. La sécurité de *Blackboard* se résume à une authentification avec nom d'usager et mot de passe. La plate-forme supporte l'ajout du protocole Kerberos afin d'offrir une authentification plus sécuritaire. De plus, un contrôle d'accès lors de l'authentification permet de donner un accès approprié aux utilisateurs. *Blackboard* ne fournit aucun mécanisme de protection pour les données emmagasinées ou transférées.

Cose 2.05

Cose (Creation Of Study Environments) a été développé par l'Université de Staffordshire. Il est un environnement d'apprentissage virtuel en Java fonctionnant entièrement sur le navigateur. Cose se veut un environnement d'apprentissage axé sur la collaboration entre étudiants et tuteurs. D'ailleurs, les outils de communication intégrés

sont le «chat», le courriel, le forum et le transfert de fichiers. Par contre, le «whiteboard» ainsi que la conférence audio et vidéo sont absents de cette plate-forme. L'accès sécurisé à Cose s'effectue avec une authentification de l'utilisateur par un nom d'usager et un mot de passe. Un contrôle d'accès est effectué lors de l'authentification afin de donner un accès en fonction du profil de l'utilisateur.

VLab

L'Université de Calgary a créé un environnement de laboratoire virtuel qu'ils ont nommé VLab. L'utilisateur peut accéder à distance au VLab et y effectuer un laboratoire. VLab se spécialise dans la simulation d'expériences aux moyens de laboratoires virtuels tel que laboratoire de chimie, laboratoire de physique, etc. Cependant, il n'offre pas de cours complets en ligne associés à leurs laboratoires virtuels. De plus, aucune sécurité particulière n'est utilisée dans le VLab. Le Tableau 2.2 résume l'évaluation des environnements d'apprentissage.

On retrouve sur Internet plusieurs laboratoires virtuels centrés sur un secteur tel que la physique, la biologie, la médecine, etc. Par contre, aucun d'eux n'offre la possibilité d'apprentissage mobile, c'est-à-dire la possibilité d'apprendre et d'effectuer des laboratoires virtuels au gré des déplacements des étudiants. En fait, jusqu'à présent, aucun n'offre de laboratoire mobile (m-laboratoire) sécuritaire. C'est dans le cadre de ce mémoire que nous allons proposer une architecture sécuritaire pour les environnements d'apprentissage mobile.

La revue de littérature de ce chapitre nous a permis de mettre en évidence les problèmes engendrés par la sécurité en général et par la mobilité des appareils qui sont l'essence même des problèmes du *e-learning*. L'objectif ultime de l'apprentissage à distance, *e-learning*, est d'améliorer et de faciliter l'accès aux ressources éducatives du monde, pour améliorer la qualité de l'éducation et de l'apprentissage. Afin d'assurer une bonne formation à distance et de bien évaluer les étudiants, il est important de s'assurer de la confidentialité, c'est-à-dire d'éviter l'interception des données (travaux)

et s'assurer de l'authentification des étudiants, c'est-à-dire d'assurer un apprentissage de qualité dans une architecture sécurisée.

Tableau 2.2 Comparaisons entre les environnements d'apprentissage

Critères	WebCT 4.1	Blackboard 6	Cose 2.05	Labo virtuel VLab
Courriel	Les étudiants peuvent utiliser l'outil de courriel interne	Les étudiants peuvent utiliser l'outil de courriel interne	Les étudiants peuvent utiliser l'outil de courriel interne	Les étudiants doivent avoir un courriel externe
«chat»	L'outil de «chat» supporte les chambres privées	L'outil de «chat» supporte les chambres privées	L'outil de «chat» supporte les chambres privées	---
«whiteboard»	Le «whiteboard» est supporté	Le «whiteboard» est supporté	Le «whiteboard» est supporté et contrôlé par l'instructeur	---
Sécurité	L'accès est protégé par un nom d'utilisateur et un mot de passe L'accès peut également être filtré par l'adresse IP. En option, le mot de passe de l'usager peut être encrypté avec SSL. Il supporte aussi Kerberos.	L'accès est protégé par un nom d'utilisateur et un mot de passe seulement. Il supporte aussi Kerberos.	L'accès est protégé par un nom d'utilisateur et un mot de passe seulement	L'accès est protégé par un nom d'utilisateur et un mot de passe seulement
Contrôle d'accès	L'administrateur peut assigner différents niveaux d'accès aux cours basés sur les rôles des utilisateurs.	L'administrateur peut assigner différents niveaux d'accès au cours basé sur les rôles des utilisateurs.	L'administrateur peut assigner différents niveaux d'accès au cours basé sur les rôles des utilisateurs.	L'administrateur peut assigner différents niveaux d'accès au cours basé sur les rôles des utilisateurs.
Prix	Le prix de la licence est basé sur le nombre d'étudiants à temps plein dans l'institution.	----	Gratuit	VLab est gratuit pour fin de recherche seulement

CHAPITRE III
ARCHITECTURE DE SÉCURITÉ POUR ENVIRONNEMENTS D'APPRENTISSAGE MOBILE

L'analyse de différentes architectures nous a permis de constater que les architectures actuelles des environnements d'apprentissage n'offrent aucun accès par réseau mobile ni d'environnement sécuritaire. C'est en constatant les faiblesses de sécurité des architectures d'environnement d'apprentissage, ainsi que leur mobilité restreinte ou inexistante, que nous avons voulu offrir de nouveaux aspects à l'architecture des environnements d'apprentissage virtuel. Ces nouveaux aspects, tels la sécurité à tous les niveaux ainsi que l'adaptation aux réseaux mobiles, assureront une évaluation efficace des étudiants, tout en leur permettant l'accès à l'environnement à n'importe quel moment et de n'importe où.

L'objectif de ce chapitre est de définir une architecture sécuritaire pour un environnement d'apprentissage mobile de type laboratoire virtuel. Le défi que pose la conception de cette architecture sécuritaire mobile demeure le choix d'une solution qui permettra de satisfaire nos exigences mais aussi qui saura s'adapter à l'évolution technologique future. Dans ce chapitre, nous analyserons les besoins de la structure de l'environnement d'apprentissage virtuel, les besoins de sécurité et de mobilité, la méthodologie utilisée et finalement nous proposerons une architecture sécuritaire et mobile.

3.1 L'apprentissage virtuel

Afin de bien traiter notre problématique, il nous apparaît essentiel de définir certains aspects nous permettant d'avoir une vue d'ensemble du sujet. Une analyse détaillée des exigences de l'environnement d'apprentissage virtuel ainsi que le rôle de chacun nous permettra de proposer une architecture adéquate.

3.1.1 Besoins de l'environnement d'apprentissage virtuel

Outre la souplesse et l'autonomie, le *e-learning* permet également de se former à moindre coût, en évitant notamment les déplacements et frais de transport, tout en individualisant les formations. Mais l'expérience montre que la réussite de la formation reste conditionnée à l'adaptation du matériel informatique et la connexion de l'apprenant à l'outil de formation. En effet, un besoin critique pour l'apprenant est l'utilisation de matériels informatiques efficaces lui permettant de bénéficier d'une qualité de service satisfaisante. L'environnement d'apprentissage virtuel doit pouvoir offrir :

- une description de cours et d'objectifs à atteindre ;
- un contenu de cours intéressant comprenant des modules qui s'enchaînent ;
- une riche base de documentation pour support à l'apprentissage ;
- une gamme d'exercices résumant les objectifs du cours ;
- des simulations intéressantes représentant le plus fidèlement possible les laboratoires traditionnels ;
- une sécurité adéquate ;
- les différents types de mobilité ;
- une collaboration étudiant-étudiant et coordonnateur-étudiant.

L'essentiel de notre architecture sera basé sur la sécurité et la mobilité lors de l'utilisation d'un environnement d'apprentissage mobile. Cette recherche ne fera pas l'évaluation pédagogique de cet environnement, mais plutôt proposera une architecture sécuritaire et mobile.

3.1.2 Acteurs de l'environnement d'apprentissage virtuel

L'environnement d'apprentissage virtuel est conçu pour offrir un contenu de cours aux apprenants tout en leur offrant un support d'apprentissage auprès d'un instructeur et des autres étudiants du même cours. Chaque acteur de l'environnement d'apprentissage virtuel accomplit des fonctions précises. Nous considérons trois acteurs : l'étudiant, le coordonnateur et le gestionnaire.

L'étudiant : il est un des utilisateurs les plus importants de l'environnement d'apprentissage virtuel. Il est donc primordial d'assurer sa satisfaction tout en lui fournissant une méthode d'accès facile, efficace et sécuritaire. L'étudiant aura accès à la consultation de toute la documentation se rapportant au cours spécifique, sans pour autant pouvoir en modifier le contenu. Par les divers outils de communication, il pourra interagir avec le coordonnateur et les étudiants de ce même cours. Par ailleurs, il aura accès à tous les outils d'apprentissage de l'environnement. De plus, l'étudiant peut être inscrit à un maximum de cours par session, ce faisant il aura un profil différent pour chaque cours. La Figure 3.1 illustre les principales actions de l'étudiant à travers l'environnement d'apprentissage virtuel.

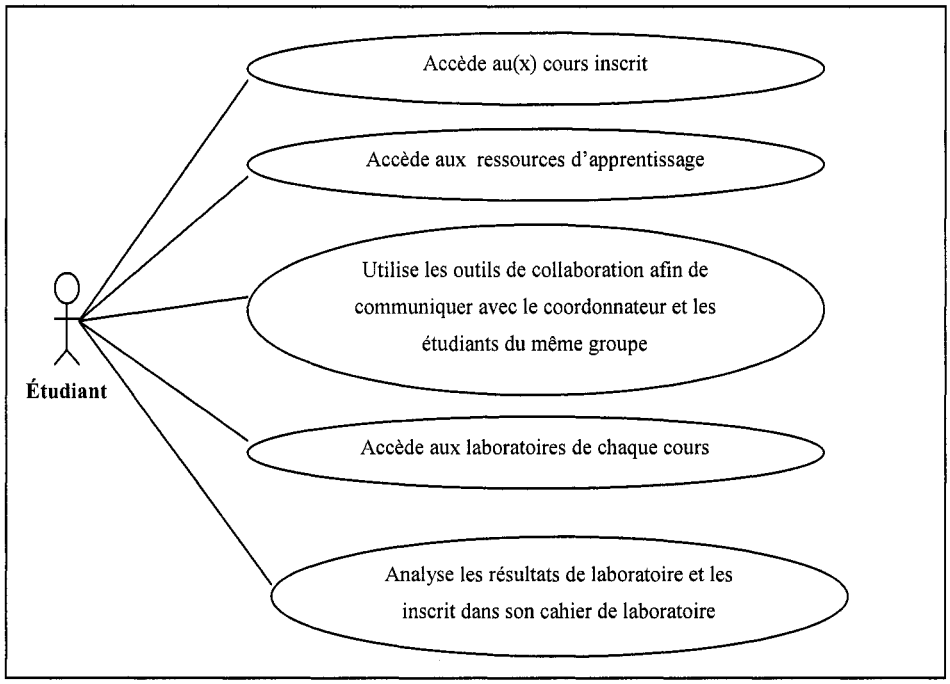

Figure 3.1 Principales actions de l'étudiant dans l'EAV

Le coordonnateur : il est celui qui supporte les étudiants tout au long de leur apprentissage afin de les amener à réaliser leurs objectifs dans un cours donné. Il a comme rôle de contrôler les discussions, répondre aux questions soulevées par les étudiants et évaluer leur travail. Il lui est aussi permis d'ajouter des objets de type texte, graphique, vidéo, audio et liens à l'environnement d'apprentissage. En fait, il se doit de

bâtir un climat de confiance dans lequel le désir d'apprendre sera nourri et augmenté. Le coordonnateur est au laboratoire virtuel ce que le professeur est à l'école traditionnelle. Le coordonnateur peut également être étudiant dans un autre cours. Ainsi, son profil sera de type étudiant pour ce cours. Cependant, l'accessibilité aux outils et services sera différente pour chaque cours. La Figure 3.2 illustre les principales actions du coordonnateur à travers l'environnement d'apprentissage virtuel.

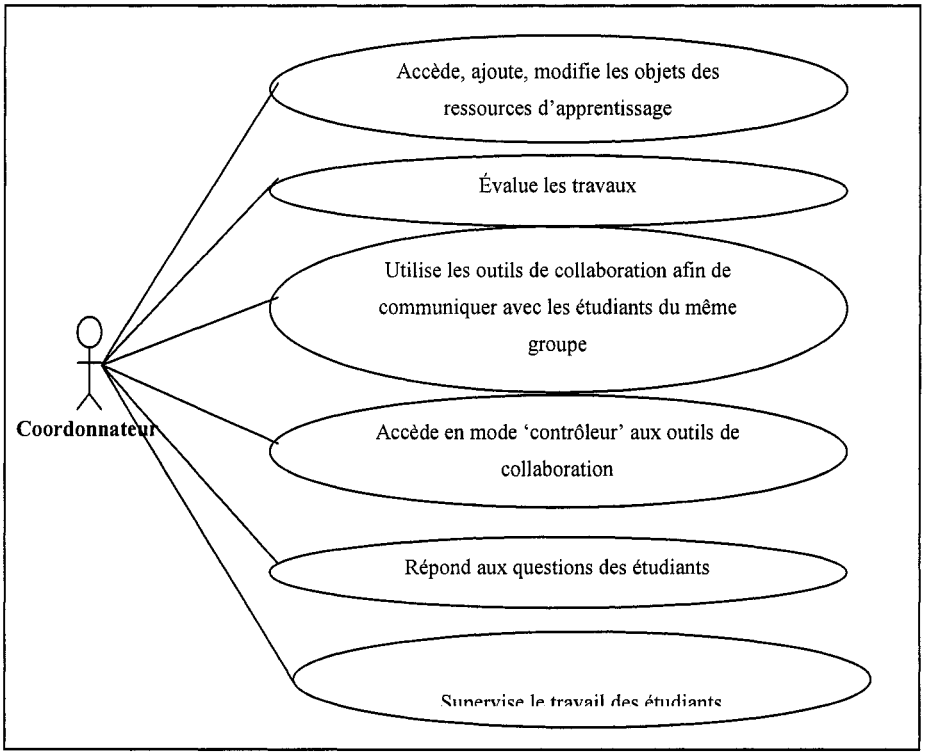

Figure 3.2 Principales actions du coordonnateur dans l'EAV

Le gestionnaire : il est responsable de la gestion des outils et services de l'environnement d'apprentissage virtuel. En collaboration avec le coordonnateur, il évalue et met à jour les services de l'environnement d'apprentissage. De plus, il gère le profil de l'étudiant et du coordonnateur. Le gestionnaire est vu comme l'administrateur système d'une école traditionnelle. La Figure 3.3 illustre les principales actions du gestionnaire dans l'environnement d'apprentissage virtuel.

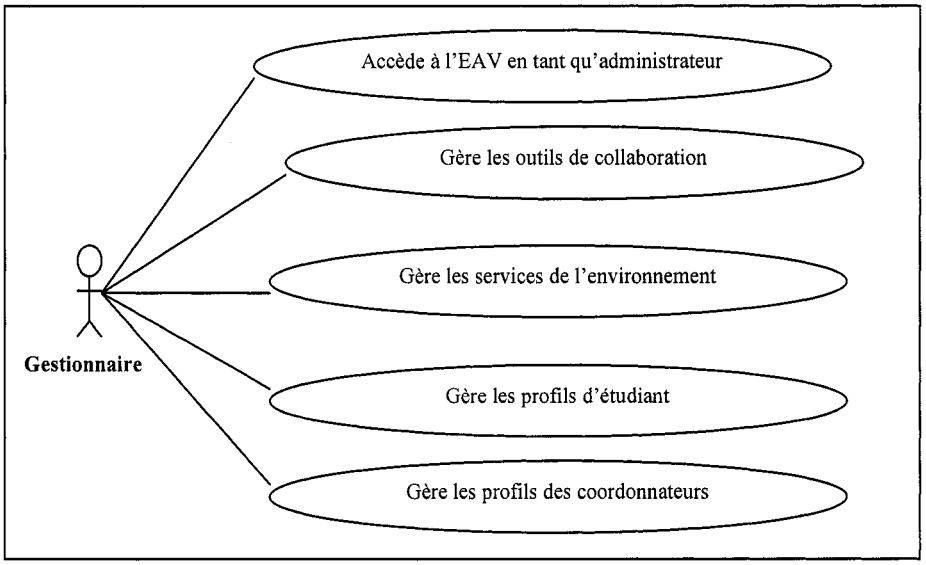

Figure 3.3 Principales actions du gestionnaire dans l'EAV

Ces trois acteurs de l'environnement d'apprentissage virtuel interagiront entre eux de différentes façons. La Figure 3.4 illustre ces acteurs dans l'environnement d'apprentissage virtuel.

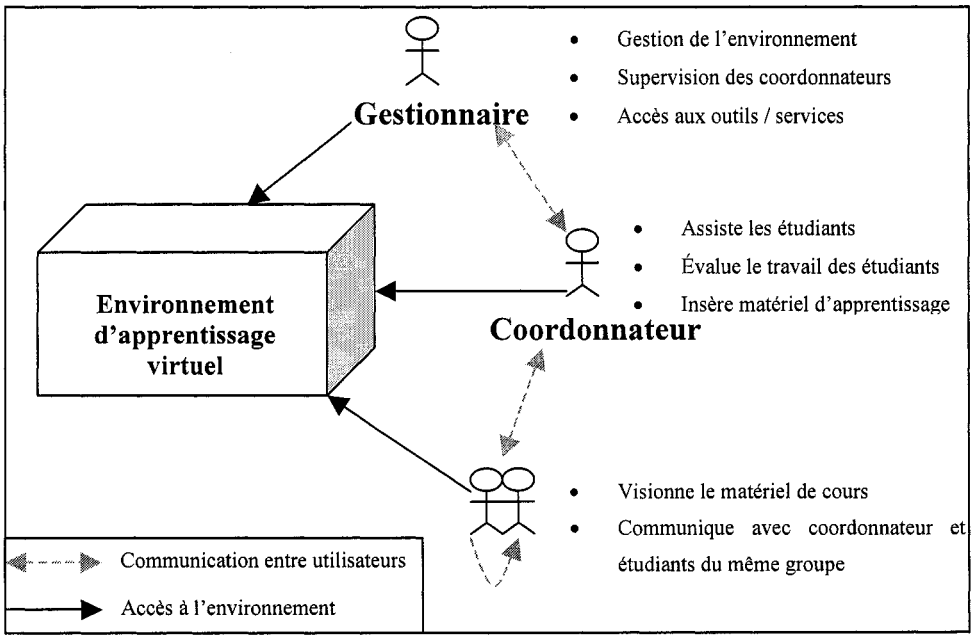

Figure 3.4 Les acteurs de l'environnement d'apprentissage virtuel

3.2 Modélisation de l'architecture proposée

Nous avons jugé bon de présenter notre approche sous forme d'encapsulation présenté graphiquement. En effet, cette méthode permet de regrouper les données et les fonctionnalités à tous les niveaux d'abstraction. Cette façon de procéder nous apporte plusieurs avantages. Elle permet :

- une bonne compréhension de l'environnement défini ;
- la réutilisation et l'extension des composantes ;
- la maximisation de la cohérence ;
- la minimisation de l'interconnexion ;
- une bonne préparation pour l'implémentation de l'architecture.

3.2.1 Diagramme de cas d'utilisation

Ce diagramme est une représentation graphique d'un ensemble de cas d'utilisation et des relations entre les acteurs et les cas d'utilisation du système d'environnement d'apprentissage. Les exigences des utilisateurs et du système, définies en début de chapitre, sont maintenant reprises de manière à être représentées par un diagramme de cas d'utilisation. Ceci permet de fournir un lien entre les exigences des utilisateurs, ceux du système, ainsi que le modèle d'architecture proposée. La Figure 3.5 présente le diagramme de cas d'utilisation pour l'environnement d'apprentissage virtuel.

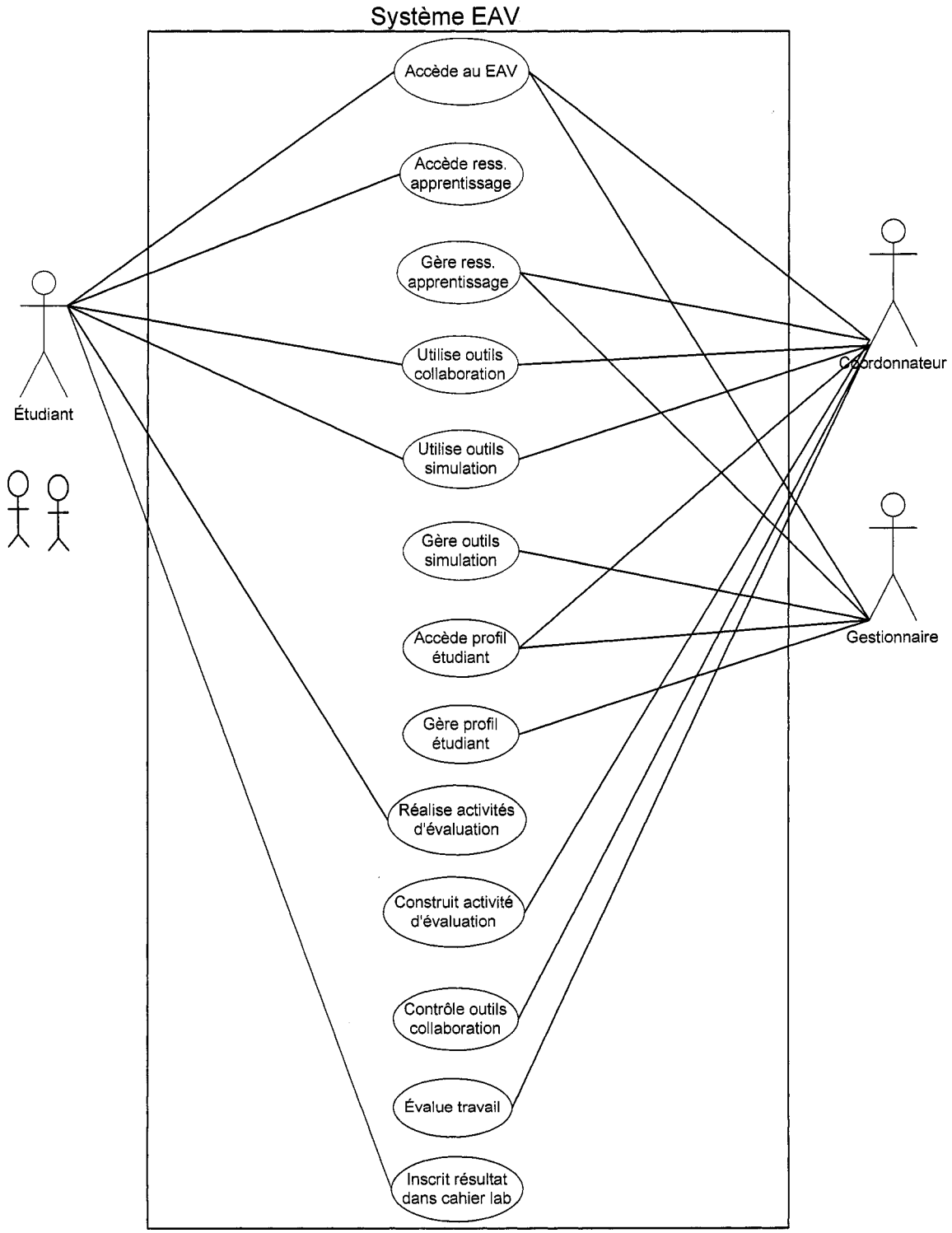

Figure 3.5 Diagramme de cas d'utilisation

3.2.2 Modèle conceptuel

Le modèle conceptuel consiste à représenter sous forme graphique les besoins des usagers. La conceptualisation nous permet d'identifier les fonctionnalités principales du de l'environnement d'apprentissage et de fournir une base à la planification de l'architecture. La Figure 3.6 est une représentation simplifiée des concepts de base de l'environnement d'apprentissage traditionnel. Ce modèle conceptuel nous permet de cibler les actions entreprises par chacun des acteurs ainsi que leur relation avec les autres objets de l'environnement d'apprentissage.

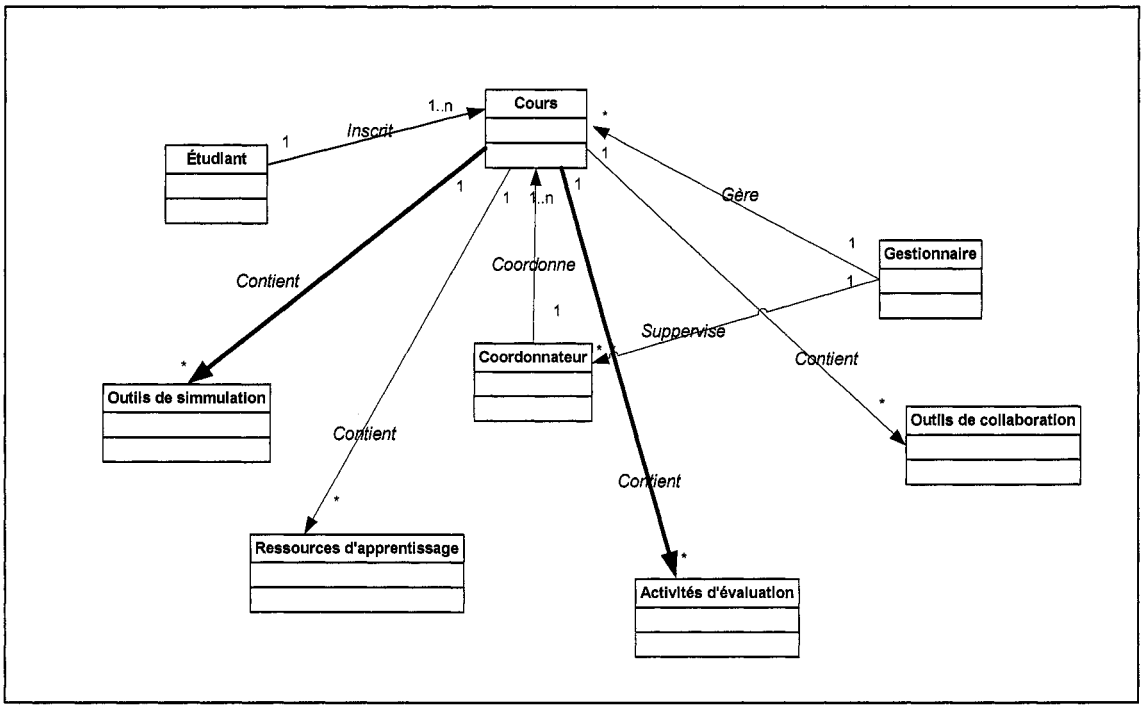

Figure 3.6 Modèle conceptuel de l'environnement d'apprentissage

À la Figure 3.6, les liens gras signifient un besoin de sécurité entre les deux objets reliés, alors qu'un lien régulier signifie qu'aucune sécurité supplémentaire n'a été ajoutée entre les deux objets reliés. De plus, à un lien est assigné un verbe d'action signifiant la relation entre les deux objets. Ainsi, les nombres inscrits sur ces liens signifient le nombre d'occurrences de l'objet en question. Par exemple, la lecture de la

relation entre l'objet étudiant et l'objet cours donne : « *un* étudiant est inscrit de *un* à *n* cours. »

3.3 Mobilité et sécurité dans l'environnement d'apprentissage

La mobilité dans l'environnement d'apprentissage virtuel est de plus en plus en demande. En effet, le campus virtuel permet de libérer les étudiants de l'attachement à une salle de cours. Nous tenons donc à offrir aux utilisateurs la possibilité de se connecter, peu importe l'endroit où ils se trouvent. Ainsi, ils pourront accéder à l'environnement d'apprentissage au moyen de PDA, téléphone cellulaire, « smart phone », ordinateur portable en plus des postes fixes, tel que présenté à la Figure 3.7.

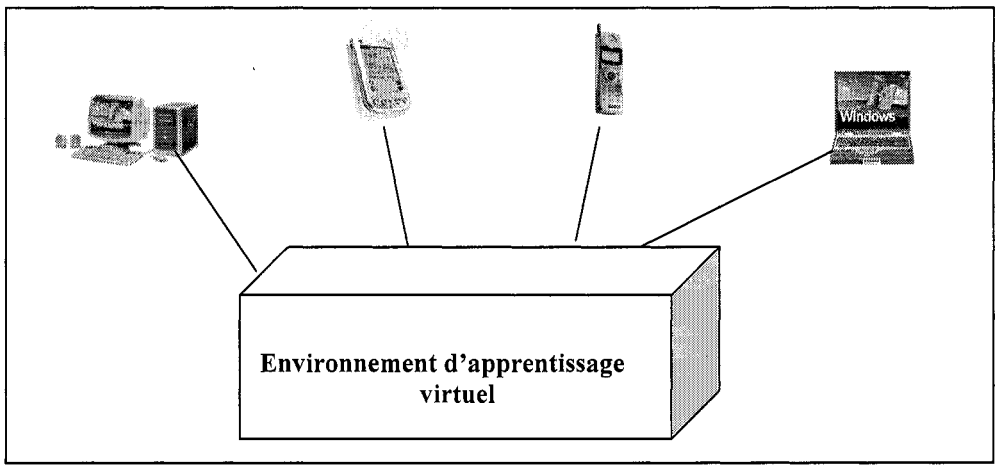

Figure 3.7. L'accès à l'environnement

3.3.1 Exigences de la mobilité

L'un des principaux objectifs visés par le *m-learning* est clairement la conception et l'expérimentation de solutions s'adaptant aux nouvelles situations d'apprentissage que la technologie génère. Cette exigence se reflète dans la nécessité de fournir des solutions flexibles qui s'adaptent aux profils variés des apprenants utilisant des appareils fixes ou mobiles.

De plus, contrairement au *e-learning*, le *m-learning* doit faire face aux capacités technologiques limitées des appareils mobiles ainsi qu'aux difficultés qu'entraîne la mobilité. La mobilité des usagers, la mobilité des terminaux, la mobilité des services

apportent leurs atouts mais entraînent aussi plusieurs contraintes dont nous traiterons dans notre architecture.

Mobilité de l'usager

D'après Floch (2001), la mobilité de l'usager doit permettre à l'utilisateur d'avoir accès à des services personnalisés avec leurs préférences et identité, indépendamment de la localisation physique du terminal et de l'équipement utilisé. Cette mobilité fait en sorte que l'usager n'est pas associé à un terminal spécifique. Il peut accéder à à ses services personnels contenus dans l'environnement d'apprentissage à partir de n'importe quel terminal mobile ou fixe disponible et de n'importe quel réseau. C'est pourquoi ce type de mobilité exige normalement qu'on identifie les usagers (identificateur personnel universel) afin qu'ils accèdent à leur environnement personnel. Dans le cas de l'environnement d'apprentissage, l'usager peut avoir accès à son environnement et accéder à ses services par l'intermédiaire de Netscape Navigator ou Internet Explorer à partir de tous les terminaux connectés sur Internet. La Figure 3.8 illustre la mobilité de la personne dans l'environnement d'apprentissage.

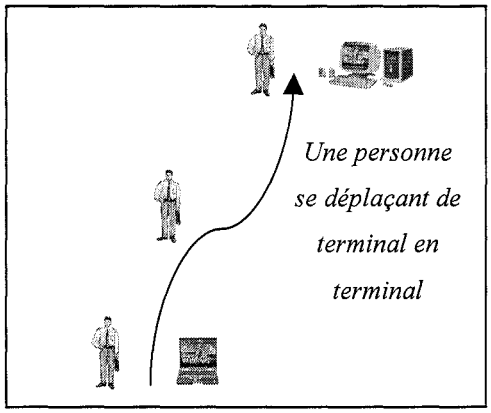

Figure 3.8 Mobilité des usagers

Mobilité des terminaux

La définition qu'en donne Pierre (2003) est la suivante : « la mobilité terminale désigne la capacité de localiser et d'identifier un terminal mobile, en permettant à ce terminal d'accéder aux services de réseau à partir de n'importe quelle position où il se trouve. » Bien entendu, l'usager doit posséder son appareil mobile et se trouver dans l'espace de couverture du réseau. La Figure 3.9 illustre la mobilité des terminaux dans l'environnement d'apprentissage.

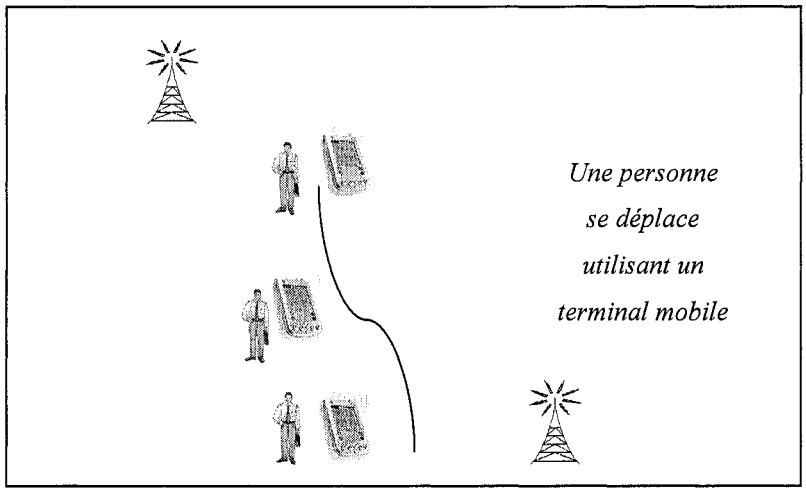

Figure 3.9 Mobilité des terminaux

La mobilité des terminaux génère quelques problèmes. Notons premièrement le problème de déplacement de l'usager avec son terminal à travers différentes zones. Par exemple, un usager accède à l'environnement d'apprentissage sur son PDA de sa maison à Montréal, puis poursuit son apprentissage tout en se déplaçant en autobus vers Toronto. L'usager s'est donc déplacé en traversant plusieurs zones. Maintenant, de quelle manière l'usager peut-il être rejoint puisqu'il ne se situe plus dans le réseau initial? Comment savoir dans quelle zone il est actuellement? La solution est l'enregistrement continuel des mouvements du terminal lorsque l'usager se déplace d'une zone de couverture à une autre. En fait, chaque zone possède un nœud de commutation gardant en mémoire l'information sur le terminal. Lorsque ce terminal quitte la zone en question, le nœud de commutation transmet l'information concernant le terminal au nœud de commutation

commutation transmet l'information concernant le terminal au nœud de commutation dans lequel l'usager se trouve à cet instant. En enregistrant à chaque instant le mouvement du terminal, le réseau peut savoir dans quelle zone se trouve le terminal et ainsi lui transmettre les données à recevoir.

Deuxièmement, notons aussi le problème de perte de connexion lors de changement de zone. Ceci se produit lorsque l'usager, utilisant son terminal dans une zone, se déplace dans une autre zone. L'entre deux zones peut faire en sorte que la connexion soit interrompue pour quelques instants. Lors d'une conversation téléphonique, cette déconnexion peut être à peine perceptible, mais peut par contre entraîner des pertes de données lors de l'utilisation de certaines applications. L'environnement d'apprentissage doit nécessairement gérer ces coupures involontaires pour éviter que l'utilisateur ne perde des données, lors de laboratoire virtuel par exemple. Le réseau doit donc garder l'état de l'utilisateur continuellement en mémoire de telle sorte que, si l'usager fait face à une coupure, il puisse se retrouver à l'endroit où il était lors de la coupure, et ainsi reprendre son apprentissage.

Finalement, le dernier problème est celui de l'interférence. Selon Mundra (1992), le processus de transmission de signaux radio dans l'air rend les systèmes sans fil vulnérables à l'interférence. Celle-ci peut être générée par d'autres produits utilisant les fréquences radio similaires dans la même zone. L'interférence dans l'environnement d'apprentissage peut se traduire par des erreurs de bits émis ou par un délai pour l'utilisateur dû au fait qu'un obstacle bloque la transmission des données sur le réseau. Pour éviter les interférences, on attribue des canaux radio différents à deux cellules voisines. La transmission doit donc changer de canal chaque fois que l'unité passe d'une cellule à une autre.

La solution envisagée pour la mobilité du terminal est l'utilisation du protocole Mobile IP. Ce protocole permet à un noeud mobile de continuer d'envoyer et de recevoir des datagrammes IP tout en utilisant une adresse fixe (son adresse initiale) même si ce nœud mobile n'est plus connecté à son réseau initial (Gupta ,1998). Ce dernier compare

le protocole Mobile IP au concept du bureau de poste qui appose une étiquette désignant la nouvelle adresse sur une enveloppe. Ainsi, celle-ci sera expédiée à la nouvelle adresse.

Mobilité des services

Selon Pierre (2001), la mobilité des services réfère à la capacité du réseau de fournir des services souscrits au terminal ou à la localisation désignée par l'usager. Cette mobilité est possible grâce à l'architecture de réseau intelligent. Gang (2001) définit un IN (Intelligent Network) comme un système intelligent qui permet de fournir de nouveaux services. Jusqu'à récemment, les réseaux de télécommunications assuraient un nombre limité de services essentiels comme la téléphonie de base, le fax et la transmission de données. Cette situation a évolué maintenant dans le nouveau contexte concurrentiel. Les opérateurs sont, en effet, conduits à diversifier, dans des délais les plus courts possibles et à moindre coût, leur offre de services auprès de la clientèle. La mobilité des services permet à l'utilisateur d'avoir accès à ses services personnels même s'il n'est pas dans son réseau d'origine. La Figure 3.10 illustre la mobilité des services dans l'environnement d'apprentissage virtuel.

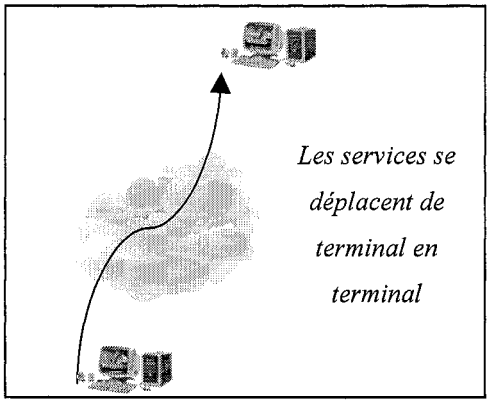

Figure 3.10 mobilité des services

La mobilité des services dépend en grande partie des caractéristiques des appareils mobiles. En effet, les limites technologiques de ces appareils apporteront des contraintes à respecter au niveau de l'architecture de l'environnement d'apprentissage. Notons quelques limites des appareils mobiles, à considérer dans certains cas :

- petit écran ;
- faible puissance du processeur ;
- interruption fréquente de connexion ;
- mémoire limitée ;
- capacité d'emmagasinage limité ;
- capacité limitée des batteries.

Certaines de ces limites peuvent affecter la mobilité des services et des applications que l'usager utilisera par l'intermédiaire de son appareil mobile. Les solutions se rattachant à la mobilité des services sont plutôt délicates. La première solution consiste à développer des services et applications s'adaptant aux limites des appareils mobiles. Par exemple, nous pouvons concevoir des applications qui se conforment à la grandeur de l'écran, des applications demandant peu de mémoire sur l'appareil mobile, etc. La seconde solution est d'imposer un minimum de capacité à l'appareil mobile.

Les limites des appareils mobiles peuvent entraîner, entre autres, un temps d'attente lors du transfert de données et un temps d'attente pour le traitement des données au cours d'un laboratoire virtuel. L'usager doit être conscient de ces limites.

Tous ces types de mobilité génèrent deux grandes contraintes : celle de la sécurité et celle de la qualité de service.

3.3.2 L'aspect de sécurité

Dans un environnement d'apprentissage, la sécurité est un aspect fondamental. Afin de sécuriser l'apprentissage de l'usager, nous devons sécuriser l'appareil, le lien qui relie l'appareil et l'environnement d'apprentissage, ainsi que le réseau de l'environnement d'apprentissage, autant pour les appareils fixes que mobiles.

Sécuriser l'appareil

La première ligne de défense est l'accès direct de l'appareil. Nous suggérons donc fortement que l'apprenant configure son appareil (fixe ou mobile) afin d'exiger un nom

d'usager et un mot de passe. Ce faisant, l'apprenant assure la sécurité d'accès de ses données ou travaux enregistrés sur l'appareil. De plus, l'utilisation d'un antivirus à jour sur chaque appareil permettra de prévenir les intrusions.

Sécuriser le lien

Le lien reliant l'appareil et l'environnement d'apprentissage doit assurer la confidentialité pour les données jugées privées de l'apprenant. En effet, l'étudiant peut vouloir transmettre son travail par courriel au coordonnateur ou à ses coéquipiers. Le paquet transmis doit non seulement garantir une certaine confidentialité afin qu'il soit indéchiffrable pour une personne autre que le destinataire, mais également respecter l'intégrité des données afin qu'elles soient inchangées durant la transmission. Par ailleurs, les réseaux sans fil qu'utilisent les appareils mobiles présentent une communication claire et ouverte à tous. Par conséquent, les informations privées transigeant sur ce lien se doivent d'être protégées.

Plusieurs solutions s'offrent à nous pour assurer la protection de la confidentialité lors du transfert. La solution la plus adaptée à l'environnement d'apprentissage est l'utilisation de SSL (Secure Socket Layer) . Il représente un canal sûr au sein de TCP/IP, où tout le trafic, entre l'apprenant et le serveur, est échangé de manière cryptée. Ceci permet de garantir la confidentialité des données, ainsi que leur intégrité. De plus, SSL est largement utilisé, donc intégré aux nouveaux logiciels. Par ailleurs, un avantage important de SSL est qu'il ne requiert aucune configuration du logiciel client (logiciel de navigation), permettant ainsi une mobilité totale sur ce point.

Sécuriser l'environnement d'apprentissage

Rendre sécuritaire l'environnement d'apprentissage signifie sécuriser la plate-forme, c'est-à-dire protéger les bases de données, les outils et services, ainsi qu'assurer la sécurité pour les différentes types de mobilité.

Bases de données

Il est impératif d'assurer l'intégrité des informations de la base de données. Ceci est effectué en contrôlant l'accès des utilisateurs par une authentification ainsi que leur type de droits sur ces données. Nous proposons, pour l'environnement d'apprentissage, un mécanisme de sécurité simple, permettant d'assurer l'authentification de façon sécuritaire, tout en favorisant la mobilité, en plus d'un contrôle d'accès effectué afin d'attribuer l'accès adéquat à l'usager, selon son profil.

De plus, il est aussi nécessaire que les bases de données possèdent une protection contre la perte des données de l'environnement. Nous optons donc pour une sauvegarde régulière sur un autre serveur situé à un endroit différent.

Outils et services

Sécuriser l'environnement nécessite de sécuriser ses outils et services. Afin de protéger l'accès aux outils et services offerts, nous assurons le contrôle d'accès sur ses outils et services. Ainsi, l'accès au site est autorisé exclusivement aux utilisateurs inscrits à l'environnement d'apprentissage. Il est donc essentiel d'instaurer une authentification des usagers lors de l'accès à l'environnement. Ceci dit, avec l'authentification de l'usager, le système sera en mesure de lui donner les accès auxquels il a droit. En fait, un profil d'usager est établi pour chaque utilisateur, en fonction de son rôle pour chaque cours. Le profil contient à la fois l'information sur l'abonné ainsi que tous les services auxquels il est inscrit. Ainsi, un usager peut avoir le rôle de coordonnateur dans un cours et avoir les droits de gestion pour ce cours, puis il peut également avoir le rôle d'étudiant dans un autre cours et posséder, dans ce cas-ci, uniquement les droits d'apprenant. Bref, l'utilisateur peut posséder plusieurs rôles dans différents cours. À chacun de ces rôles est attribué un profil d'utilisateur lui donnant les accès appropriés. En plus du contrôle d'accès effectué sur les outils et services lors de l'utilisation des outils de communications, nous assurons la confidentialité, l'intégrité et la non-répudiation par des options de sécurité à sélectionner par l'utilisateur.

Mobilité

Mais qu'advient-il de la sécurité reliée à la mobilité? L'usager mobile se heurte à un plus grand nombre de contraintes de sécurité que l'usager utilisant un appareil fixe. Analysons maintenant la sécurité que requièrent les différents types de mobilité.

Sécurité face à la mobilité des usagers

Le concept de mobilité de la personne entraîne certaines complications dans la sécurité, principalement au niveau de la confidentialité. L'usager peut laisser des traces sur les terminaux qu'il utilise, en négligeant de supprimer la copie de son travail par exemple. En effet, lorsque l'usager utilise un terminal commun à plusieurs, il faut pouvoir assurer une confidentialité des données appartenant à chaque personne visitant ce terminal. Ainsi, dans l'environnement d'apprentissage, l'usager aura une section « espace utilisateur » où il pourra travailler et sauvegarder ses travaux et ses notes. Il faut néanmoins sensibiliser l'usager à la suppression de ses données personnelles lors de visites sur un terminal commun.

Sécurité face à la mobilité des terminaux

La principale complication au niveau sécurité qui est introduite par le concept de la mobilité des terminaux, est le déplacement à travers les différents réseaux. En effet, ce déplacement est possible grâce aux ondes radio accessibles à tous. Un usager peut communiquer des données avec un coéquipier et celles-ci peuvent être captées par d'autres usagers dans la même zone. Il faut donc donner la possibilité à l'usager de rendre sa communication sécuritaire. La façon utilisée dans l'environnement d'apprentissage est de crypter, par un mécanisme tel que SSL, les communications privées telles que lors de l'authentification, lors de l'accès au cahier de laboratoire et de l'envoi de courriel. Par exemple, au moment de l'envoi d'un message courriel, l'utilisateur aura à choisir l'option confidentialité-intégrité, et/ou l'option signature électronique. La première option lui permettra d'envoyer son courriel de manière

cryptée, puis la seconde lui permettra d'envoyer son courriel en prouvant qu'il est bien le rédacteur.

Sécurité face à la mobilité des services

La mobilité des services entraîne certaines contraintes de sécurité, car les services doivent être accessibles par les usagers en mouvement en provenance de différents réseaux. L'authentification devient donc importante. Il faut pouvoir s'assurer que l'usager demandant les services est bien inscrit à ces services. L'authentification doit être fiable, facile d'utilisation, tout en assurant la sécurité lors de la mobilité.

Les utilisateurs de l'environnement d'apprentissage requièrent des besoins spécifiques en sécurité lors de l'utilisation des outils et services du système. Ces utilisateurs exigent une plus grande sécurité pour certaines applications plutôt que d'autres. Ceci nous amène à proposer des niveaux de sécurité adaptés à leurs besoins. Nous tenons donc à ajuster le niveau de sécurité en fonction de l'outil ou du service utilisé. Par exemple, une sécurité plus accrue sera instaurée lors d'un envoi d'un travail au coordonnateur, contrairement à celle utilisée lors de la consultation de la documentation liée au cours.

Certaines fonctions de l'environnement d'apprentissage demandent un degré de sécurité plus élevé que d'autres. Le Tableau 3.1 présente la relation entre les fonctions et le type de protection proposé.

Authentification

Il est important d'identifier les utilisateurs (étudiant, coordonnateur, gestionnaire) avant qu'ils joignent l'environnement d'apprentissage virtuel. L'authentification est la base des exigences de sécurité pour l'apprentissage à distance.

Nous devons donc adéquatement identifier l'étudiant de manière à s'assurer que celui qui accède au système est bien celui qu'il prétend être. Afin d'identifier les usagers, nous optons pour un nom d'utilisateur ainsi qu'un mot de passe défini par l'usager.

Tableau 3.1 Relation entre les fonctions et le type de protection

Fonctions	Actions	Type de protection				
		A	C	I	NR	CA
Administration	Accès et modification du profil	X	X	X		X
	Ajout, modification, suppression des données de l'environnement	X		X		X
Apprentissage	Lecture	X				X
	Ajout, modification, suppression de la documentation	X		X		X
Outils de simulation	Effectuer un laboratoire	X	X	X		X
Outils de communication	Public	X				X
	Privé	X	X	X	X	X
Activités d'évaluation	Effectuer un test ou contrôle	X	X	X	X	X

A : Authentification C : Confidentialité I : Intégrité NR : Non-répudiation
CA : Contrôle d'accès

Il est important d'assurer un degré de sécurité élevé pour l'authentification des usagers, car le coordonnateur et le gestionnaire ont accès à plusieurs fonctions cruciales (modification et destruction) de l'environnement d'apprentissage. Entre autres, les étudiants ont accès au matériel de cours, aux outils d'apprentissage ainsi qu'à leur profil. Afin d'assurer une sécurité plus stricte, nous pourrions proposer l'utilisation d'une authentification de type PKI (Public Key Infrastructure). Par contre, avec ce type de sécurité, une clé privée serait alors insérée dans l'appareil de l'étudiant, ce qui réduirait le concept de mobilité des personnes, en obligeant celles-ci à n'utiliser que l'appareil possédant la clé. Nous optons donc pour une connexion SSL lors de l'authentification à l'environnement d'apprentissage car elle permet de chiffrer l'authentification lors de son transport sur le réseau.

De plus, afin d'assurer une sécurité adéquate, la désactivation de l'accès de l'étudiant sera effectuée à chaque fin de trimestre. Ceci assurera un contrôle d'authentification pour les étudiants actifs uniquement.

Considérant que plusieurs usagers peuvent utiliser un ordinateur public, nous proposons qu'après un temps donné d'inutilisation la session devienne inactive, afin de permettre l'utilisation par un autre étudiant. Ainsi, l'étudiant initial devra effectuer à nouveau son authentification.

Confidentialité

La confidentialité a comme objectif d'assurer que les données ou messages transmis ne peuvent être accessibles par une personne non autorisée. Dans l'environnement d'apprentissage, certaines données sont privées et ne doivent en aucun cas être accessibles par les utilisateurs réguliers. Nous devons donc assurer la confidentialité des cahiers de laboratoire, des profils étudiants et profils coordonnateurs, en plus de certaines communications par « chat », courriel et «whiteboard ».

En effet, par l'utilisation des outils de collaboration, l'étudiant devrait pouvoir poser des questions en privé au coordonnateur et être assuré que la discussion reste privée. Une connexion SSL peut être utilisée de façon à construire un tunnel sécuritaire entre l'étudiant et le coordonnateur. Toutes les communications circulant dans ce tunnel seront chiffrées assurant ainsi la confidentialité de la communication.

Les cahiers de laboratoire d'étudiants sont accessibles uniquement par l'étudiant lui-même. Il suffit à l'étudiant d'une authentification pour entrer dans son environnement personnel d'apprentissage. À ce moment, il aura accès aux cahiers de laboratoire des cours auxquels il est inscrit. En fait, chaque apprenant accède uniquement à son matériel d'apprentissage.

Intégrité

L'intégrité consiste à assurer que le message n'ait pas été modifié pendant sa transmission et que le message arrivant au destinataire est bien celui qui a été envoyé par l'émetteur. L'intégrité dans l'environnement d'apprentissage est essentielle. Les étudiants doivent avoir la certitude que les données sont exactes et non pas été modifiées, et ce, autant pour les utilisateurs d'appareils mobiles que pour les utilisateurs d'appareils fixes. L'intégrité des données peut être maintenue par l'utilisation du message *Digest* lors de la connexion SSL. En fait, ce message correspond à une empreinte digitale des données. Concrètement, SSL calcule le *Digest* du message et appose ce *Digest* à l'intérieur des données chiffrées avant de l'envoyer au destinataire. Lorsque le message arrive à destination, SSL calcule à nouveau le *Digest* basé sur les données reçues et compare avec le *Digest* apposé au message. Ainsi, si les deux *Digest* ne correspondent pas, cela indique que les données ont été corrompues, et de ce fait, elles ne seront pas envoyées à l'application. Ce mécanisme garantira l'intégrité des données de façon « end to end ».

Non-répudiation

La non-répudiation consiste, lors d'un échange, à assurer le destinataire d'un message que l'émetteur est bien celui qu'il prétend être et à l'émetteur que le destinataire a bien reçu le message. Dans le cas d'un environnement d'apprentissage traditionnel, l'étudiant note son nom, son numéro de matricule et porte sa signature sur ses travaux afin de s'identifier correctement. Ensuite, il remet en main propre son travail au professeur, s'assurant ainsi que ce dernier l'a bien reçu. Nous devons faire en sorte que l'environnement d'apprentissage virtuel assure la non-répudiation au même titre que l'environnement d'apprentissage traditionnel, et ce, malgré les contraintes technologiques. En fait, nous devons lier le document à l'émetteur et au récepteur afin que personne ne désavoue ses actions ou ne nie qu'un échange a eu lieu. Nous croyons que la meilleure solution pour assurer la non-répudiation est d'utiliser les signatures électroniques. La signature électronique peut être effectuée par un outil tel que PGP.

L'utilisation de la signature électronique nous permet d'assurer intégrité et la non-répudiation des documents envoyés.

Contrôle d'accès

Dans une classe traditionnelle, le professeur contrôle l'accès à la salle de cours lui-même, en laissant entrer seulement les étudiants qui sont inscrits au cours. C'est ce que nous devons appliquer dans l'environnement d'apprentissage virtuel. En fait, le contrôle d'accès consiste à appliquer des filtres dans le monde réel (clés, carte magnétique, ...) et des filtres dans le monde virtuel (garantir que seuls les flux autorisés transitent).

Nous devons également procurer un contrôle d'accès virtuel en nous assurant que les fonctions de création, modification et suppression, ainsi que les sections privées (notes, travaux, profil étudiant, profil coordonnateur) sont accessibles uniquement par les administrateurs (coordonnateur et gestionnaire). Nous devons également nous assurer que les étudiants ont un accès en lecture seulement, sans aucune possibilité de modification ou suppression de données.

Le contrôle d'accès se fera lors de la création d'un nouveau compte utilisateur. Les accès sont attribués selon le profil de l'usager : étudiant, coordonnateur ou gestionnaire pour chaque cours auquel il s'inscrit.

Différentes fonctions et mécanismes de sécurité sont installés dans l'environnement d'apprentissage. Ils seront appliqués afin de sécuriser l'information circulant entre l'entité *étudiant*, l'entité *évaluation* et l'entité *note*. En utilisant un mécanisme de chiffrement, nous allons sécuriser la transmission entre:

- ✓ l'entité cours et l'entité activité d'évaluation ;
- ✓ l'entité activité d'évaluation et l'entité note ;
- ✓ l'entité cours et l'entité note ;
- ✓ l'entité activité de simulation et l'entité cours ;
- ✓ l'entité activité de simulation et l'entité note.

Nous devons également considérer un mécanisme de communication sécuritaire pour les outils de collaboration. La sécurité de communication n'étant pas nécessaire à chaque utilisation, nous offrons un mécanisme de sécurité optionnel sur chaque outil de collaboration. Ainsi, l'apprenant peut sélectionner l'option pour avoir une communication privée (seulement entre l'émetteur et le récepteur) et/ou sélectionner l'option pour une communication chiffrée et/ou pour l'utilisation de la signature électronique. Ceci permet de procurer aux utilisateurs le choix de sécurité pour chacun des outils de communications, sans compromettre le réseau et la sécurité.

3.3.3 Scénarios

Connaissant les besoins des utilisateurs, les limites de la sécurité et de la mobilité, ainsi que les modules de notre architecture, nous pouvons maintenant élaborer différents scénarios. Les scénarios permettent de définir les étapes des différentes actions de l'environnement d'apprentissage. Nous nous contentons de définir deux scénarios : l'étudiant discutant d'un travail avec des coéquipiers de façon sécuritaire par courriel, l'étudiant exécutant un laboratoire virtuel.

a) Courriel sécuritaire entre coéquipiers

Les étudiants forment une équipe afin de réaliser le travail de groupe. Ils ne forment le groupe qu'avec des étudiants appartenant au même cours et même groupe. Une fois le groupe formé, ils peuvent communiquer par «chat», courriel, «whiteboard» et vidéo-conférence. Le scénario présente l'utilisation de l'outil de communication courriel sécurisé. Les Figures 3.11 et 3.12 représentent le scénario d'envoi d'un courriel sécuritaire. Dans cette figure, l'authentification de l'étudiant a été acceptée. Il est actuellement dans le laboratoire du cours, prêt à communiquer avec ses coéquipiers par courriel, sous une communication chiffrée.

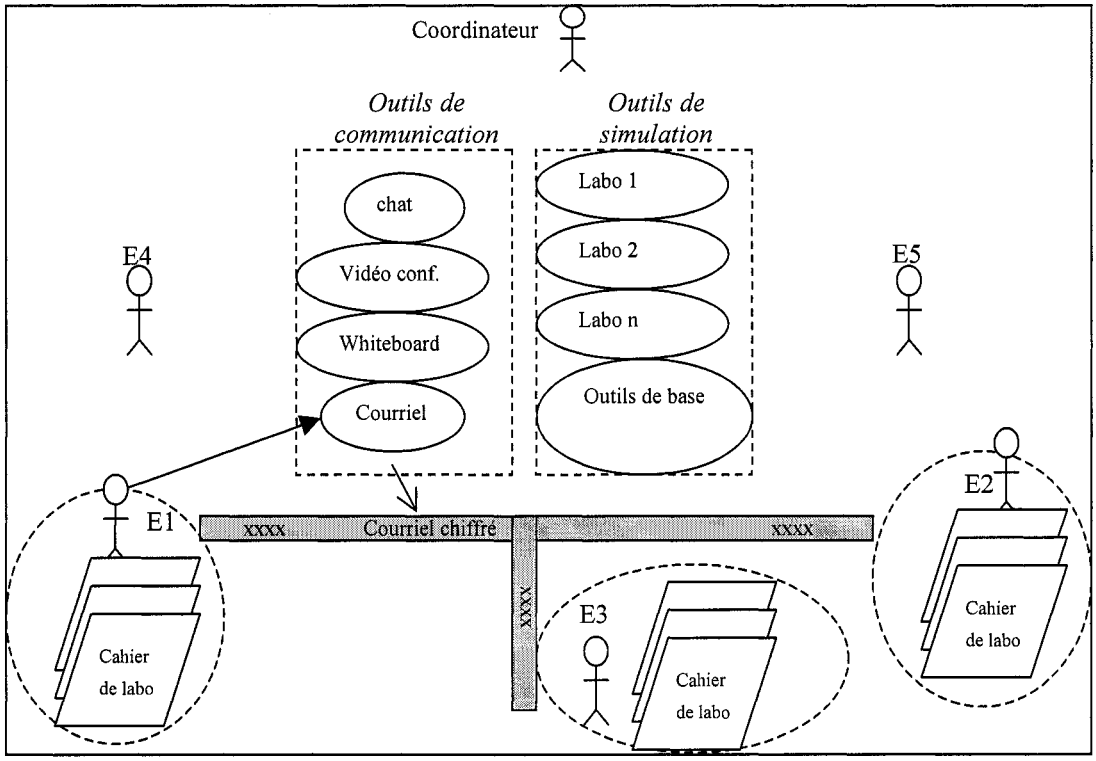

Figure 3.11 Vue générale du scénario d'envoi de courriel sécuritaire

b) Laboratoire

Les apprenants effectuent le laboratoire correspondant au cours auquel ils sont inscrits. Lors de l'exécution du laboratoire, les apprenants ont accès parallèlement aux outils de base des laboratoires tels que : calculatrice, cahier de note, table de conversion, etc. De plus, le laboratoire virtuel peut être utilisé en combinaison avec les outils de communication. Ainsi, l'apprenant peut poser des questions via les outils de communication synchrones et asynchrones au coordonnateur et aux étudiants appartenant au même groupe uniquement. En accédant aux outils synchrones («chat», «whiteboard» et vidéo- conférence), l'apprenant peut voir les autres étudiants de son groupe qui sont actuellement en ligne sur le site d'environnement d'apprentissage.

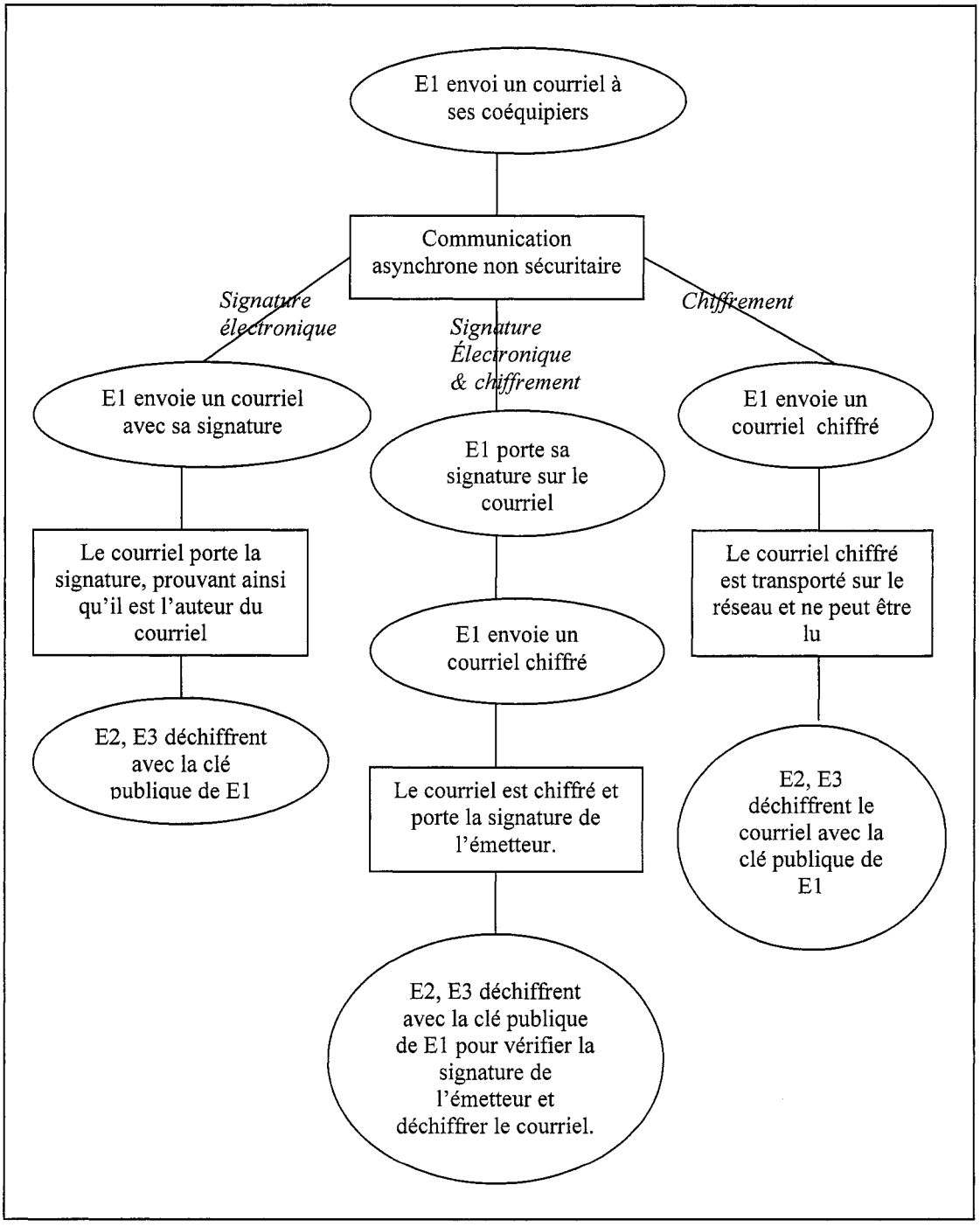

Figure 3.12 Étapes du scénario d'envoi de courriel sécuritaire

Les Figures 3.13 et 3.14 représentent le scénario d'exécution d'un laboratoire.

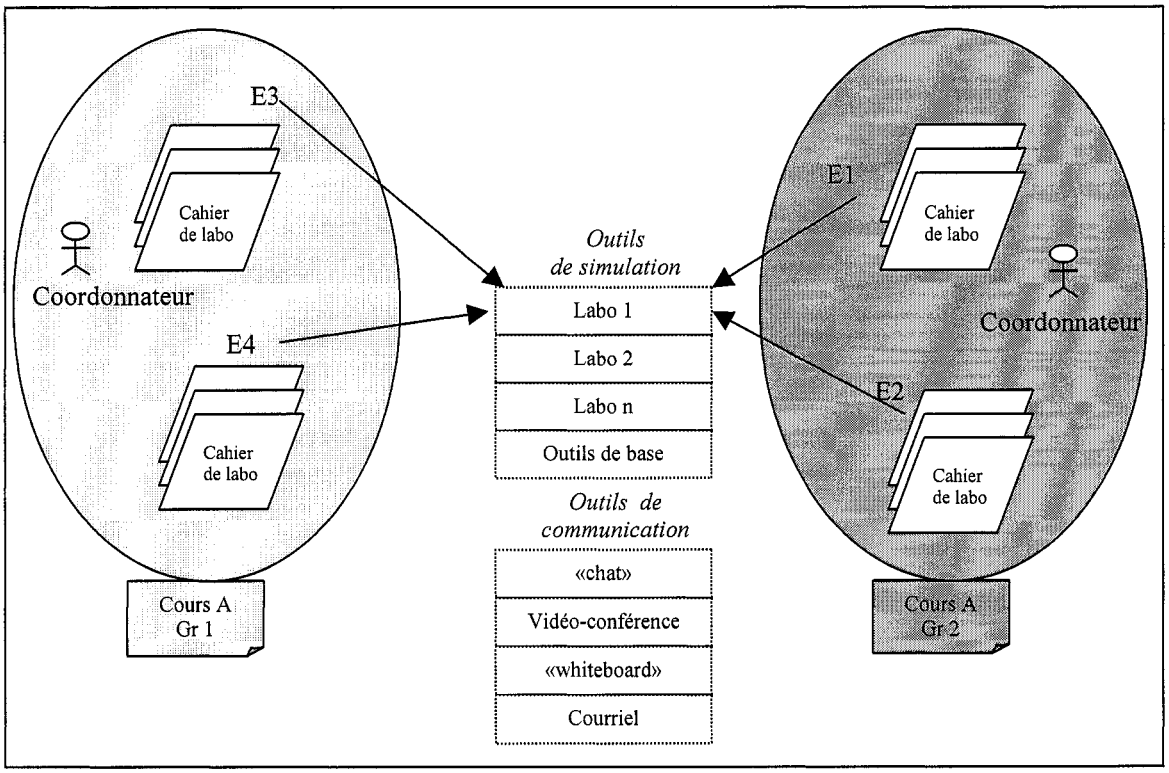

Figure 3.13 Vue générale du scénario d'exécution d'un laboratoire

3.4 Qualité de service

Il est difficile de nos jours de concevoir une solution adaptée aux besoins de chaque application. Pour ce faire, nous devons fournir un service mettant des techniques à la disposition de chaque application, afin de répondre aux exigences des applications et des utilisateurs. Ce service doit être générique et adaptatif, car les critères de qualité de service peuvent être différents d'une application à l'autre. De même, ces critères peuvent aussi être contradictoires, étant donné qu'ils ne peuvent être tous satisfaits à la fois ; ainsi, un compromis s'impose.

Les caractéristiques de la qualité du service (QdS) réseau sont généralement exprimées par les critères suivants:

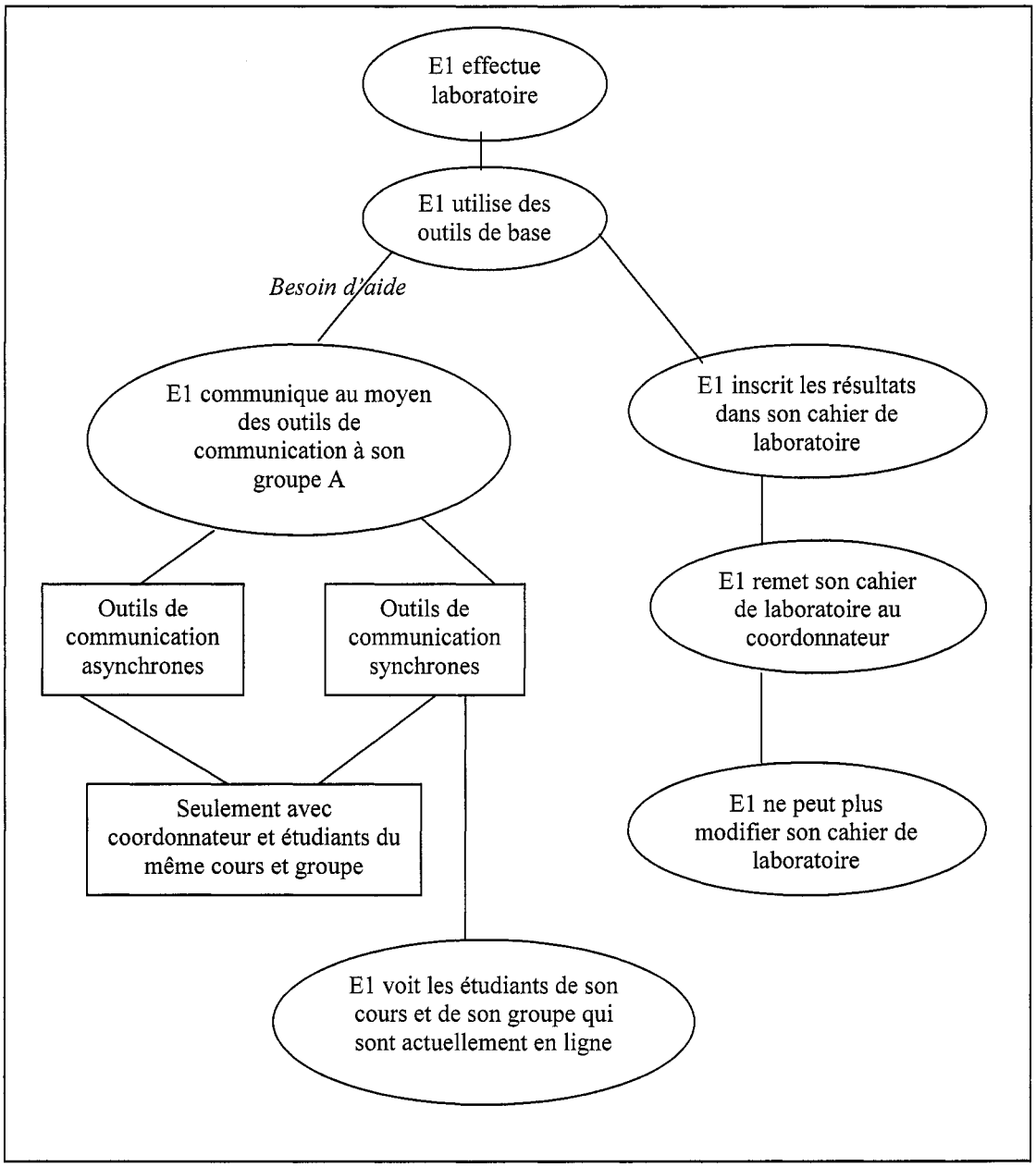

Figure 3.14 Étapes du scénario d'exécution d'un laboratoire

Délai: temps écoulé entre l'envoi d'un paquet par un émetteur et sa réception par le destinataire. Le délai tient compte du délai de propagation le long du chemin et du délai de transmission induit par la mise en file d'attente des paquets dans les systèmes intermédiaires.

Gigue : variation du délai de bout en bout.

Bande passante ou débit maximum: taux de transfert maximum pouvant être maintenu entre deux points terminaux.

Disponibilité : taux moyen d'erreurs d'une liaison.

Plusieurs facteurs peuvent avoir un impact sur ces critères. Observons maintenant quels sont ceux reliés à l'environnement d'apprentissage virtuel.

3.4.1 Qualité de service dans un laboratoire virtuel sécuritaire et mobile

L'environnement d'apprentissage virtuel possède des besoins spécifiques en terme de QdS. En effet, nous devons tenir compte de certaines exigences relatives à ce type d'environnement. Notons entre autres la priorité de certaines applications, le débit de transmission pour l'outil de conférence et la minimisation des pertes.

Certaines applications de l'environnement d'apprentissage possèdent un plus grand niveau de priorité que d'autres, afin de garantir le service. Par exemple, lors de simulations, l'utilisateur interagit avec des instruments de mesures précis. Ces applications de simulation étant importantes dans le processus d'application et d'évaluation, nous leur assurons une priorité afin de ne pas perdre les données mesurées lors de la simulation. Ainsi, les commandes aux instruments et les mesures reçues sont transférées au travers du réseau de manière prioritaire, de façon à réduire la perte de ce type de paquet même si le réseau est en état de congestion.

La qualité de service face à la mobilité diffère de la qualité de service traditionnel. En effet, le mouvement de l'appareil affecte la qualité de service. Selon Chalmers (1999), la clé du concept dans la gestion de la qualité de service pour les environnements mobiles est l'adaptation au changement de qualité de service. Ainsi, certaines situations telles que le déplacement entre les stations du réseau sans fil, les effets de l'environnement et les trous noirs (sous les ponts, tunnel, ...) affectent la qualité de service. Le résultat est une courte perte de communication probablement imperceptible pour la communication vocale, mais dans l'environnement d'apprentissage, il peut en résulter une perte de données pour certaines applications. Il nous faut donc gérer

dynamiquement la qualité de service des appareils mobiles tout en gérant les déconnexions, en permettant à l'usager de se reconnecter et de se retrouver à l'endroit où il a été déconnecté.

L'environnement d'apprentissage virtuel offre des fonctions multimédias (voix sur IP, vidéo-conférence) qu'on veut absolument fournir aux usagers des réseaux sans fil. Cependant, ces services multimédia consomment beaucoup de ressources et n'utilisent pas efficacement et équitablement le support de communication qu'ils doivent partager avec des services de données. Afin de fournir équitablement et efficacement des services multimédias ainsi que des services de données aux utilisateurs, on doit utiliser des mécanismes assurant une certaine qualité de service spécifique à chaque type d'application. De ce fait, on introduit un mécanisme de QdS au niveau des couches supérieures afin d'allouer une certaine bande passante et une certaine priorité pour chaque type d'application. Alors, le mécanisme de QdS DiffServ apparaît idéal pour assurer une qualité de service dans les environnements d'apprentissage virtuel.

DiffServ

La couche liaison de données ne peut pas distinguer entre les natures des flux (audio, vidéo, données). C'est pourquoi nous devons ajouter la qualité de services *DiffServ* (Diffenrentiated Service) au niveau des couches réseau et transport afin de différencier entre ces différents flux. *DiffServ*, défini au niveau 3 du modèle OSI, repose sur un modèle simplifié dans lequel le trafic qui entre dans le réseau est classé. Les paquets, identifiés par leur point de code DSCP (DiffServ Codepoint) marqué en amont, recevront un traitement préférentiel par le réseau. Le principe consiste à allouer une bande passante prioritaire à certains types d'application. Ainsi, dans l'environnement d'apprentissage, on fixera une priorité pour l'audio, la vidéo et les données relatives aux laboratoires virtuels plus importants que toute autre donnée. Par contre, nous utiliserons CBQ (Class Based Queuing) qui est un mécanisme permettant d'éviter qu'une seule classe de trafic ne monopolise les ressources.

3.5 Architecture globale

Dans les sections précédentes, nous avons illustré par des diagrammes les besoins des apprenants en terme de sécurité et de mobilité tout en tenant compte des limites de ceux-ci. Cela nous a permis de bien cibler les exigences et les limites afin de proposer une architecture adaptée à l'environnement d'apprentissage virtuel. L'architecture globale est présentée à la Figure 3.15 suivie de la description de chaque module.

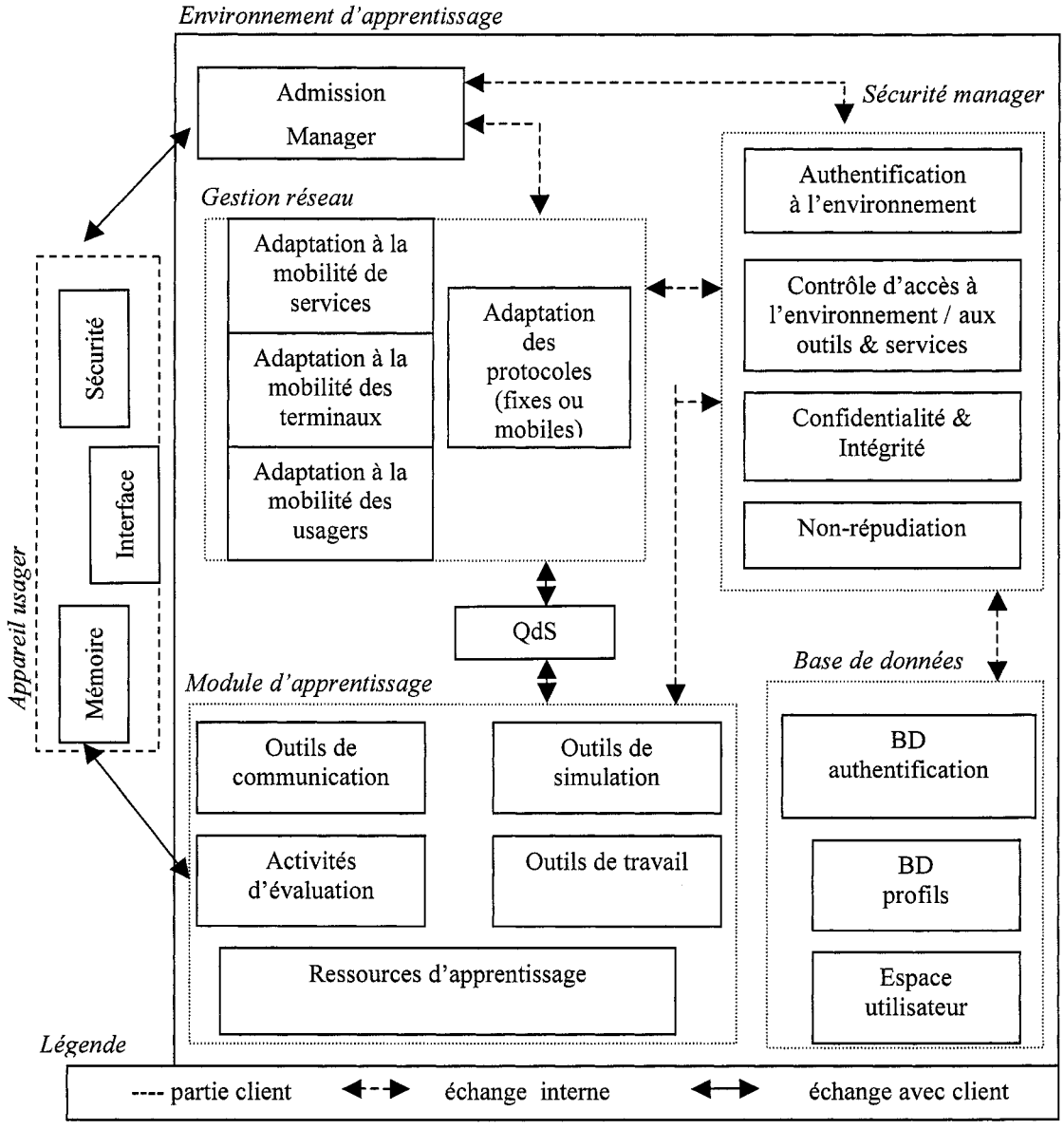

Figure 3.15 Architecture globale

Appareil usager : Cette section correspond à l'appareil que l'usager utilise pour accéder à l'environnement d'apprentissage. Cet appareil peut être mobile ou fixe. Il comprend trois modules dont la mémoire qui se réfère à la mémoire vive de l'appareil, l'interface qui est l'écran par lequel l'usager visionne ses apprentissages et la sécurité qui comprend le programme anti-virus recommandé sur chaque appareil.

Admission Manager : Ce module permet de gérer l'authentification des usagers accédant au site. Une fois l'authentification reçue de l'usager, ce module vérifie avec la base de données d'authentification, tout en passant par le module de sécurité qui cryptera le mot de passe lors de la vérification. Si l'authentification correspond à celle de la base de données d'identification, l'usager accède au site d'apprentissage selon son profil, sinon l'accès au site lui est refusé.

Gestion réseau : Ce module comprend deux sections dont la première est l'adaptation aux protocoles selon un appareil fixe ou mobile. Cela signifie que l'usager accède au site d'apprentissage en utilisant un protocole particulier. L'environnement adapte ce protocole afin qu'il puisse interagir avec l'ensemble de l'environnement d'apprentissage. La deuxième section est celle de la mobilité. Chacun de ces modules de mobilité est géré de façon à offrir la mobilité de service, la mobilité des usagers et la mobilité des terminaux.

Module d'apprentissage : Ce module comprend cinq sous-modules dont des outils de communication, des outils de simulation, des activités d'évaluation, des outils de travail ainsi que des ressources d'apprentissage. Ces modules sont accessibles directement par les apprenants en fonction des cours inscrits, par les coordonnateurs et par le gestionnaire. Chacun de ces modules est adapté au profil de l'usager de manière à ce que l'usager puisse accéder uniquement aux outils auxquels il est autorisé.

Outils de communication : ce module comprend les outils permettant la communication entre les étudiants de même cours ainsi que la communication entre les étudiants et le coordonnateur du cours. Les outils qui permettrent cette communication sont : le courriel, le «chat», la vidéo-conférence et le «whiteboard». À chacun de ces outils, l'usager peut y ajouter un mécanisme de sécurité tel que le cryptage, la signature électronique ou simplement établir une conversation fermée pour le «chat», la vidéo-conférence et le «whiteboard». Il faut noter que le module des outils de communication est accessible en tout temps dans l'environnement d'apprentissage.

Outils de simulation : Ce sous-module inclut tous les outils de simulation de l'environnement d'apprentissage, dont les différents types de laboratoire virtuel.

Outils de travail : Ce module compte les outils spécifiques de chaque laboratoire tel que la calculatrice scientifique, l'oscilloscope, l'ohm-mètre, etc.

Activité d'évaluation : Ce sous-module permet d'évaluer les connaissances de l'apprenant par différentes activités telles que le test, le quiz et l'énoncé de travaux. Ces activités varient en fonction des exigences du cours choisi. Les activités telles que le quiz et le test ne sont qu'une forme d'évaluation personnelle, ainsi les résultats de ces activités ne sont pas comptabilisés.

Ressources d'apprentissage: Ce sous-module comprend l'ensemble des ressources d'apprentissage disponibles pour l'apprenant. Notons entre autres, les notes de cours, les présentations, les documentations manuscrites et Web correspondante à chaque cours.

Base de données des profils : Ce sous-module inclut les profils de chacun des utilisateurs inscrit en tant qu'apprenant ou coordonnateur. L'information contenue dans les profils est le type d'utilisateur (étudiant, coordonnateur ou gestionnaire) ainsi que l'information personnelle à son sujet telle que l'adresse, le numéro de téléphone, les

cours inscrit, les cours réussis,... Lorsque l'usager est authentifié, l'environnement vérifie son profil (type d'utilisateur) afin de lui donner les droits d'accès appropriés. Il faut noter qu'un usager peut être à la fois étudiant pour un certain nombre de cours et coordonnateur pour d'autres cours.

Base de données d'authentification : Ce sous-module comprend tous les noms d'usager ainsi que les mots de passe de chaque utilisateur. Un contrôle d'accès strict permet d'assurer la confidentialité des informations contenues dans les bases de données et de faire en sorte que seul le gestionnaire peut y avoir accès.

Espace utilisateur : Ce sous-module est réservé aux documents d'apprentissage personnel de chaque utilisateur. Il comprend, entre autres, les travaux et le cahier de laboratoire.

Sécurité manager : Le module de sécurité collabore avec chacun des modules de l'environnement d'apprentissage virtuel afin d'offrir des fonctions de sécurité. En effet, il offre différentes fonctions de sécurité afin de sécuriser soit l'environnement d'apprentissage (la plate-forme) soit la communication.

Authentification à l'environnement : Ce sous-module procure la sécurité lors de l'authentification de l'usager. Ainsi, le mot de passe et le nom d'utilisateur sont cryptés afin d'assurer la confidentialité tout au long du processus d'authentification.

Contrôle d'accès à l'environnement / aux outils & services : Ce sous-module gère l'accès aux outils et services. En fait, il donne à l'usager l'accès à l'environnement et aux outils et services selon le type d'utilisateur.

Confidentialité & Intégrité : Ce sous-module assure la confidentialité et l'intégrité des données lors de l'utilisation des outils ou services en offrant une connexion SSL pendant l'utilisation des outils de simulation et d'activités d'évaluation. La confidentialité

demeure le choix de l'usager lors de l'utilisation des outils de communication. Il peut sélectionner ou non l'option confidentialité. De plus, il gère la sauvegarde régulière des données jugées importantes sur un serveur distant.

Non-répudiation : La non-répudiation relève du choix de l'usager lors de l'utilisation des outils de communication (courriel). Il peut sélectionner l'option non-répudiation afin d'insérer sa signature électronique sur son envoi, assurant ainsi le récepteur qu'il est bien le rédacteur du message.

Qualité de service : Ce module maintient une qualité de service adéquate pour le module de gestion de réseaux et le module d'apprentissage.

CHAPITRE IV
IMPLÉMENTATION ET RÉSULTATS

Comme tout modèle conceptuel, notre architecture permet d'étendre la portée des laboratoires virtuels en y apportant l'aspect sécuritaire, tout en supportant la mobilité. Après une description de notre architecture sécuritaire mobile au chapitre précédent, nous allons maintenant présenter son implémentation. Le grand défi que pose la conception demeure le choix des mécanismes de sécurité pouvant s'adapter non seulement aux différents types de mobilité, mais encore à l'évolution des technologies futures. Dans cette perspective, ce chapitre présente la démarche suivie pour la conception de l'architecture. Nous décrivons tout d'abord les détails de l'implémentation concernant les approches utilisées. Par la suite, nous présentons l'implémentation de l'environnement sécuritaire mobile. En dernier lieu, nous proposons des simulations effectuées pour évaluer l'implémentation ainsi que les résultats obtenus.

4.1 Détails d'implémentation

Pour effectuer cette implémentation, nous utilisons le langage Java. Ce langage purement orienté objet a été choisi pour plusieurs raisons, dont la principale est la portabilité. En effet, la portabilité de Java réside dans le fait qu'il peut tourner sur n'importe quelle machine disposant d'un interpréteur Java. Cette portabilité est fondamentale dans notre environnement d'apprentissage basé sur Internet, où un nombre important de machines et systèmes d'exploitation différents inondent ce milieu. Les langages C et C++ sont plus difficilement portables puisqu'ils autorisent l'usage de pointeurs pour adresser directement des portions de mémoire et ne gèrent pas automatiquement la désallocation de la mémoire.

L'implémentation et les mesures ont été réalisées au LARIM (Laboratoire de Recherche en Réseautique et Informatique Mobile) à l'École Polytechnique de Montréal. Nous avons utilisé le réseau local LAN Ethernet 100 Mbps, mais également le réseau local sans fil IEEE 802.11b configuré en mode infrastructure. Les expériences ont été effectuées sur un réseau privé au sein du LARIM et ont été divisées en deux groupes. Le premier porte sur les tests dans un réseau câblé, et le second sur les tests effectués dans un réseau sans fil. Pour le premier groupe de tests, le réseau comportait deux machines dont un serveur et un client. Les machines utilisées sont dotées d'un processeur Pentium IV à 1.80 GHz possédant 785.712 koctets de mémoire vive pour le serveur et Pentium IV à 1.80 GHz possédant 261.424 koctets de mémoire vive pour le client.

L'environnement logiciel du client est composé de :

- WebPerformance 2.6 permettant de simuler des connexions HTTP et HTTPS.
- Navigateur Internet Explorer 6.0.

L'environnement logiciel du serveur est composé de :

- Système d'exploitation Windows 2000 ;
- Environnement et machine virtuelle Java : JDK 1.3.1 inclus dans le kit Borland Jbuilder 7.0 ;
- Environnement de développement : Borland Jbuilder 7.0, incluant (Java virtual Machine), environnement graphique et librairies de développement ;
- JWSDP 1.3 (Java Web Services Developer Pack) incluant JSSE 1.0.3 et Apache Tomcat ;
- Java Secure Socket Extension (JSSE 1.0.3) permettant l'implémentation des protocoles SSL et TLS ;
- Serveur Web Apache Tomcat 4.0.3 inclus dans JWSDP 1.3 ;
- Application Web représentant l'environnement d'apprentissage virtuel.

Afin de mesurer la performance de l'architecture, nous avons utilisé le logiciel WebPerformance Testing (WPT). En fait, WPT se place entre le navigateur client et le serveur Web. Il mesure les flux HTTP ou HTTPS émis par le serveur Web aux requêtes du navigateur client. Il permet de créer plusieurs usagers virtuels afin de mesurer le temps de réponse de l'application Web et la charge du serveur.

Au moment de la création d'une simulation, le WPT nous permet de sélectionner :

- ✓ la durée du test ;
- ✓ la vitesse du réseau ;
- ✓ le nombre d'usagers virtuels à simuler ;
- ✓ l'augmentation des usagers virtuels à toutes les X minutes ;
- ✓ la période d'enregistrement des données recueillies.

La Figure 4.1 présente l'écran du WPT lors de l'enregistrement d'une simulation.

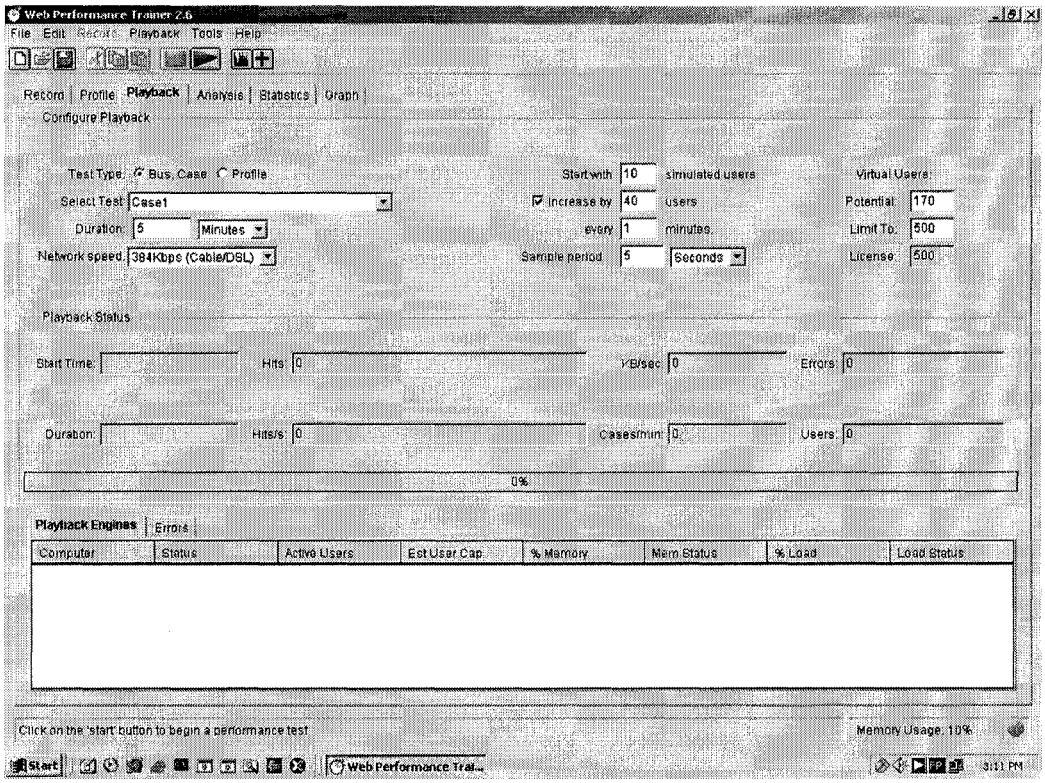

Figure 4.1 Enregistrement d'une simulation de WPT

Nous avons installé et configuré certains appareils afin d'utiliser le réseau sans fil IEEE 802.11b du LARIM. Nous avons d'abord installé une carte réseau sans fil sur le poste client, puis installé et configuré un Access point Cisco relié au serveur Web. Nous avons disposé notre poste client dans un rayon de cinq mètres de l'accès point. Nous avons également créé un réseau privé 192.168.1.00, réservé uniquement pour notre trafic. La Figure 4.2 illustre l'environnement d'apprentissage mobile.

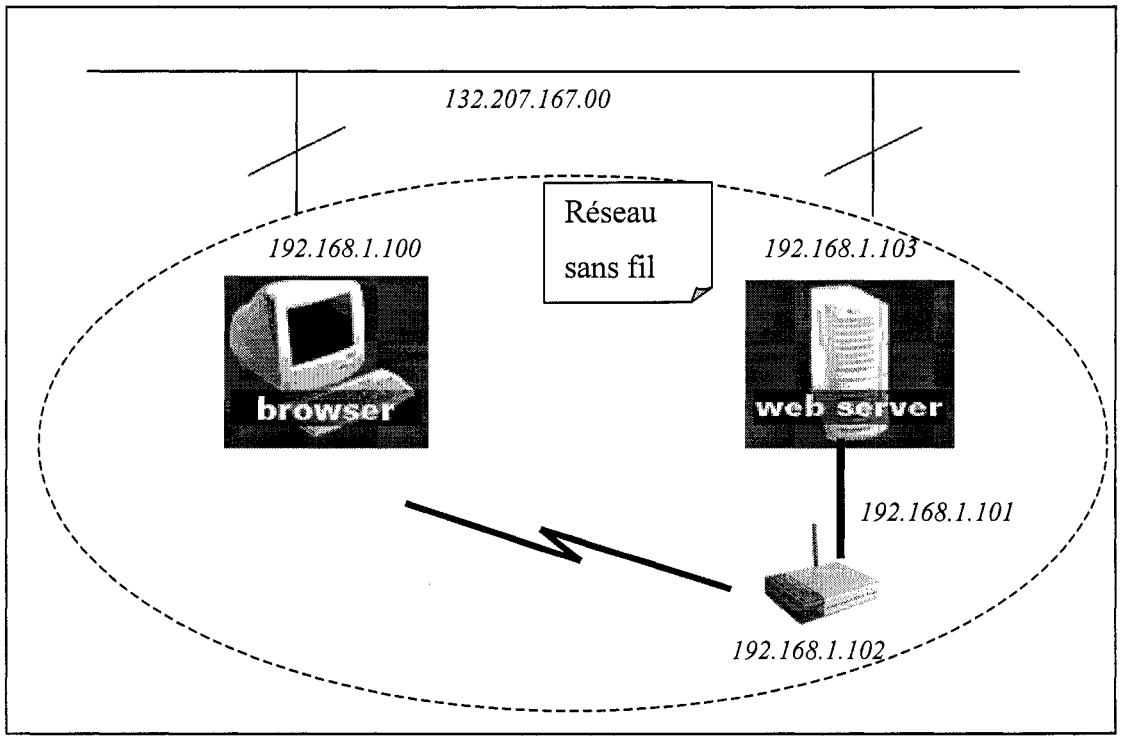

Figure 4.2 Environnement d'apprentissage mobile

Nous avons choisi de relier par câble l'accès point au serveur, de façon à ne pas utiliser la bande passante de l'accès point réservé pour les clients.

La sécurité dans l'environnement d'apprentissage intègre deux aspects : la sécurité reliée au réseau et la sécurité reliée à la plate-forme.

Sécurité reliée au réseau

Environnement câblé

Nous avons utilisé le protocole de sécurité SSL afin de rendre sécuritaires les échanges de données par l'intermédiaire des applications Web de l'environnement d'apprentissage virtuel. Le protocole SSL fait appel aux versions de cryptage haute performance des navigateurs offerts par Microsoft et Netscape. Il utilise différents algorithmes de cryptage (RSA, MD5,...) lors de l'authentification, du transfert des données, de la transmission des certificats et l'établissement des clés de session. L'utilisation de SSL nous permet de sécuriser la communication entre le client et le serveur grâce à l'application Web de notre environnement câblé.

Environnement sans fil

Plusieurs problèmes de sécurité avec le protocole WEP ne permettent pas de considérer cette option comme étant sécuritaire. Les solutions possibles sont EAP (Extensible Authentification Protocol), WPA (Wi-Fi Protected Access) ou IEEE 802.11i. WEP2 n'est pas à considérer car, selon Labiod (2002), WEP2 possède toujours des failles. Ces solutions reposent sur la sécurité de l'accès au réseau sans fil, ainsi que sur le chiffrement des données transigeant sur le réseau.

Notre objectif est de sécuriser l'ensemble de l'environnement d'apprentissage qui se trouve être une application Web. Ainsi, l'information à sécuriser ne se situe qu'entre l'application Web client et l'application Web serveur. La solution sécuritaire demeure alors le protocole SSL. Il nous permet de rendre sécuritaire notre environnement câblé et notre environnement sans fil.

Il faut noter que SSL ne peut être installé sur les appareils mobiles de type PDA ou cellulaire à cause de sa taille. L'architecture WAP des appareils mobiles utilise le protocole WTLS qui est semblable à SSL. Il nous faut donc installer un Proxy à l'intérieur du serveur Web afin de faire la conversion entre WTLS et SSL. Évidemment, le procédé de conversion est transparent à l'utilisateur d'appareil mobile. Ainsi, du côté client, nous avons uniquement un Web navigateur utilisant SSL ou WTLS (pour PDA ou

cellulaire) pour sécuriser les communications de l'environnement d'apprentissage virtuel. Le fait d'avoir une simplicité de sécurité du côté client apporte une grande mobilité pour l'usager.

Sécurité reliée à la plate-forme

Afin d'implanter une sécurité adéquate dans l'environnement d'apprentissage virtuel, nous croyons qu'en plus de sécuriser la communication, nous devons sécuriser la plate-forme de l'environnement d'apprentissage virtuel. Nous avons pu renforcer la sécurité de la plate-forme en protégeant l'accès aux bases de données, au serveur et aux outils.

Nous protégeons l'accès à la base de données des profils, où l'on retrouve les cahiers de laboratoire, par une authentification. L'accès est donc restreint aux apprenants, enseignants et administrateur de l'environnement qui peuvent uniquement consulter et modifier leur propre profil. Seul l'administrateur du système possède tous les droits sur les profils utilisateurs. Il en est de même pour la base de données d'authentification.

Nous avons aussi limité l'accès physique au serveur Web ainsi qu'aux bases de données en les plaçant dans une salle fermée à clé.

4.2 Implémentation de l'environnement d'apprentissage virtuel

Étant donné l'objectif de notre recherche, nous n'avons pas jugé pertinent ni essentiel de concevoir l'environnement d'apprentissage dans son ensemble. Nous avons donc conçu trois fonctions typiques de l'environnement d'apprentissage virtuel intégrées dans une application Web. Ces fonctions sont : la recherche d'information concernant un cours, l'authentification, et la recherche dans le cahier de laboratoire.

4.2.1 Recherche de cours

La recherche de cours comporte la description des cours offerts, les crédits et les préalables. Elle est disponible pour tous sur le site Web de l'EAV du LARIM. La recherche de cours représente l'ensemble des navigations HTML des utilisateurs sur

l'environnement d'apprentissage virtuel. Selon Barford (1999) la distribution du volume des pages Web est exprimée par un log normal .

Ainsi, nous avons construit la recherche de cours en nous basant sur la distribution générale des pages Web, afin de représenter le plus possible l'ensemble des navigations HTML. De cette façon, nous avons construit trois pages HTML ayant un volume de 30 Ko, de 300 Ko et une dernière de 1 Mo. Les figures 4.3 à 4.5 illustrent la recherche de cours construite dans l'application Web.

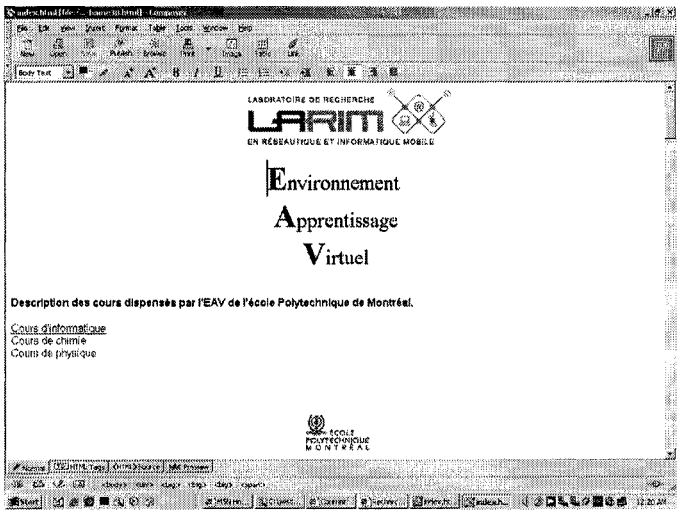

Figure 4.3 Description de cours (30 Ko)

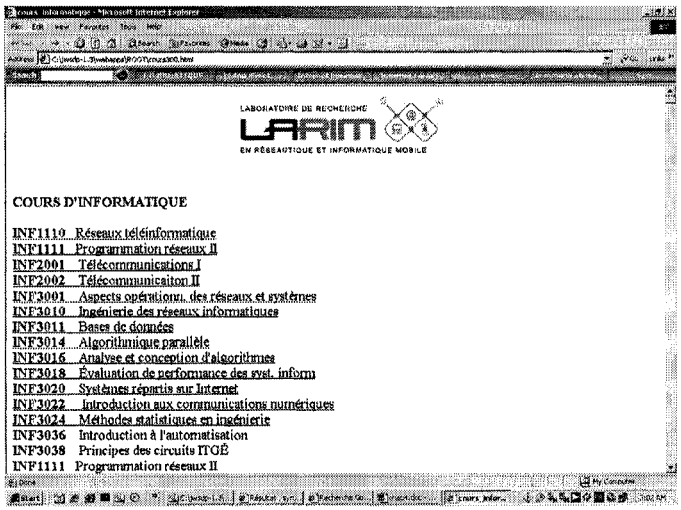

Figure 4.4 Description de cours (300 Ko)

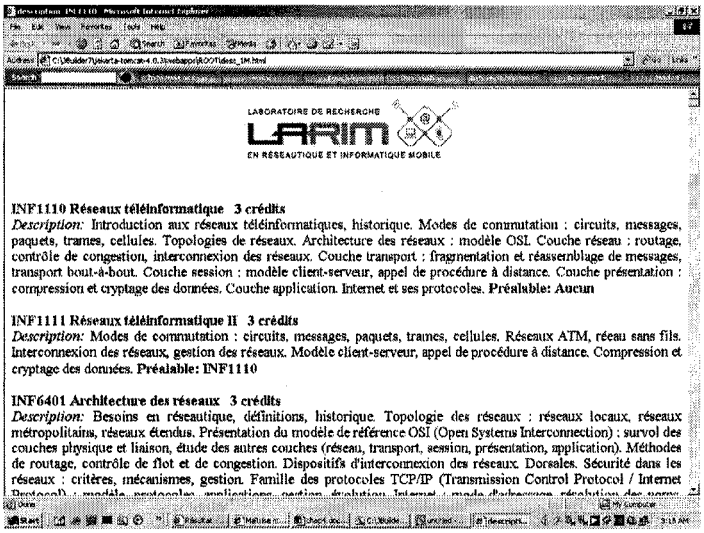

Figure 4.5 Description de cours (1 Mo)

4.2.2 Authentification

La fonction d'authentification permet l'accès à l'environnement d'apprentissage seulement aux personnes autorisées. L'authentification est construite avec un servlet qui consulte une base de données de mots de passe. L'authentification est effectuée avec le protocole SSL de façon à crypter l'information transportée. L'utilisateur entre en premier lieu son nom d'usager et son mot de passe, tel que présenté à la Figure 4.6.

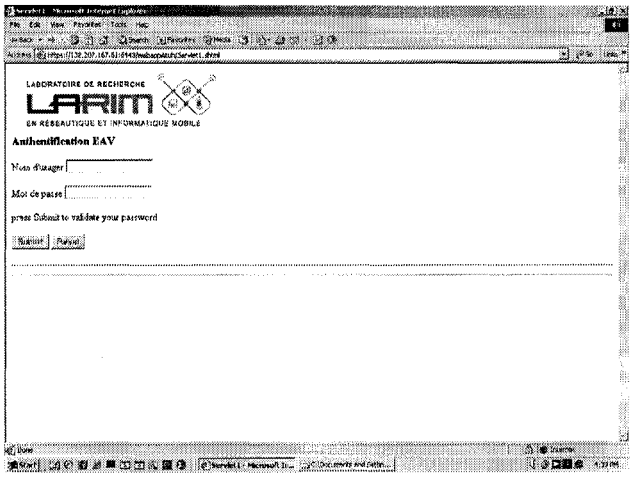

Figure 4.6 Page d'authentification

Par la suite, le nom d'usager et le mot de passe sont cryptés et envoyés au serveur qui les compare à ceux de la base de données. Le processus d'authentification se déroule comme l'illustre la Figure 4.7.

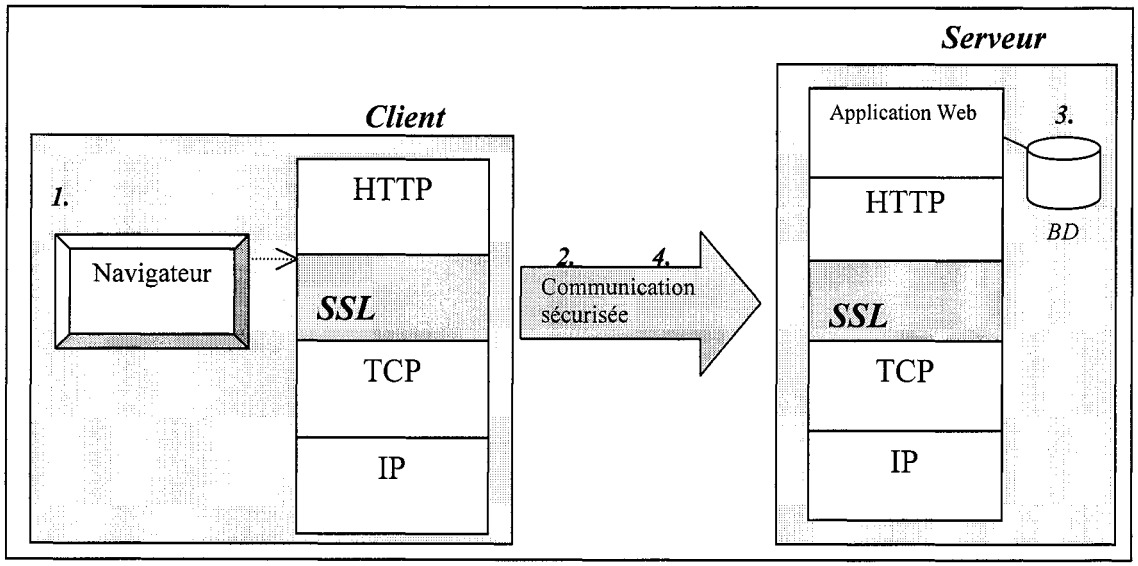

Figure 4.7 Utilisation de SSL dans l'authentification

1. Le client (étudiant) inscrit son nom d'usager et son mot de passe dans la page authentification ;
2. a) Le client se connecte au serveur par l'intermédiaire du port 8440 (SSL) ;
   b) Le serveur envoie son certificat contenant la clé publique ;
   c) Le client accepte ou non le certificat du serveur ;
   d) Le client crée une clé aléatoire et utilise la clé publique du serveur pour la chiffrer ;
   e) Le client envoie la clé au serveur ;
   f) Le serveur déchiffre la clé et utilise la clé aléatoire du client afin de créer une clé de session secrète ;
   g) Le client et le serveur utilisent la clé de session secrète pour leur communication ;
   h) Le client reçoit la page sécurisée demandée de l'application Web ;

3. L'application Web accède à la base de données afin de vérifier l'authentification ;
4. Le serveur renvoie une page d'accès autorisé ou non autorisé.

4.2.3 L'accès à un cahier de laboratoire

Le cahier de laboratoire est un élément essentiel à l'étudiant dans l'environnement d'apprentissage virtuel. En fonction des types d'exercices reliés à un cours, le volume du cahier peut varier. Lors de nos simulations, nous avons évalué un cahier de laboratoire de 30 Ko afin de bien voir l'effet de la sécurité sur le volume du cahier de laboratoire. La Figure 4.8 représente un cahier de laboratoire (30 Ko) d'un étudiant en informatique.

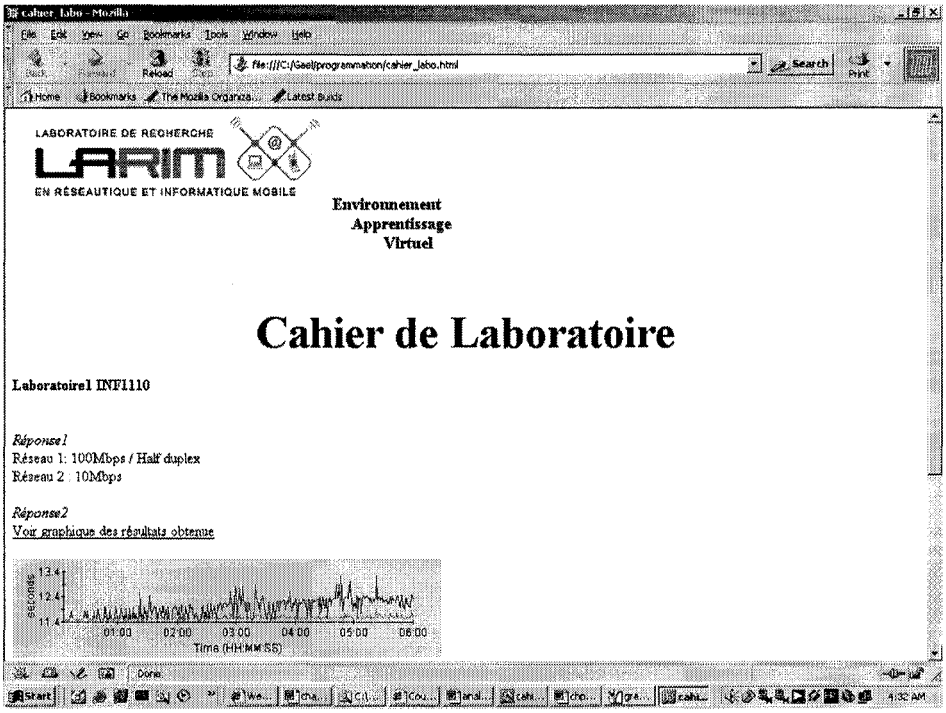

Figure 4.8 Cahier de laboratoire 30 Ko

L'accès au cahier de laboratoire représente la consultation du cahier de laboratoire de l'étudiant sur le réseau. L'étudiant s'étant déjà authentifié, il peut maintenant avoir accès à ses cahiers de laboratoire. Cette fonction est construite avec un servlet qui accède à la base de données des cahiers de laboratoire. Elle utilise le protocole SSL defaçon à

crypter l'information qui transige entre le client et le serveur, sécurisant ainsi les données du cahier de laboratoire de l'étudiant.

4.3 Simulation et résultats

Dans cette section, nous présentons les métriques utilisées pour l'évaluation de la performance à travers le plan d'expériences. Nous présenterons ensuite les types de simulations produites et les résultats de nos mesures, pour ensuite établir une comparaison de la performance dans un environnement câblé sécuritaire et mobile sécuritaire. Nous étudierons les métriques choisies dans un environnement mobile avec sécurité et sans sécurité, afin de tirer une conclusion sur notre architecture sécuritaire.

4.3.1 Plan d'expérience

Cette section présente les métriques utilisées pour l'évaluation de la performance de notre architecture sécuritaire dans un environnement mobile. Afin d'évaluer la performance de la sécurité de notre plate-forme de télécommunications, nous avons proposé quelques scénarios d'expérimentation. La performance de la sécurité dans l'environnement d'apprentissage virtuel sera évaluée en analysant certaines métriques lors de la recherche de cours, de l'authentification, ainsi que de l'accès à un cahier de laboratoire.

Métriques

Nous utiliserons deux métriques de performance dans notre évaluation :

- La *Charge du serveur* qui consiste à mesurer la quantité de requête HTTP / HTTPS reçue et traitée par le serveur durant l'utilisation des mécanismes de sécurité ;
- Le *Temps de réponse* qui consiste à mesurer le délai encouru pour qu'une requête reçoive une réponse lors de l'utilisation des mécanismes de sécurité. Le calcul du temps débute au moment où la requête s'établit sur le poste client et se termine lorsque le client reçoit la réponse à sa requête.

Cependant, certains paramètres propres au système peuvent influencer les métriques mentionnées ci-dessus. Le Tableau 4.1 illustre les facteurs influençant les métriques.

Tableau 4.1 Identification des facteurs

Facteurs	Type	Nom	Niveau
1-Sécurité d'un service	Facteur primaire et contrôlable	Aucune sécurité	Aucune sécurité
		Sécurité	Application du mécanisme de sécurité approprié
2-Mobilité d'un service	Facteur primaire et contrôlable	Aucune mobilité	Environnement câblé
		Mobilité	Environnement mobile

Facteur 1

Niveau 1 :

Mesurer les métriques lorsqu'aucun mécanisme de sécurité n'est implanté dans l'environnement d'apprentissage virtuel à travers un réseau mobile WLAN.

Niveau 2 :

Mesurer les métriques lors de l'utilisation des mécanismes de sécurité dans l'environnement d'apprentissage virtuel à travers un réseau mobile WLAN.

Facteur 2

Niveau 1 :

Mesurer les métriques lorsqu'aucune mobilité n'est permise, c'est-à-dire dans un environnement câblé de type Ethernet à 10 Mbps.

Niveau 2 :

Mesurer les métriques dans un environnement mobile de type WLAN (IEEE 802.11b).

4.3.2 Simulations

Pour chaque simulation dans l'environnement câblé et mobile, nous avons spécifié le nombre d'utilisateurs virtuels créés et le temps de la simulation. Nous avons limité les utilisateurs virtuels à un maximum de 35 sur une période de 1 minute.

4.3.2 Résultats et analyse

a) Environnement câblé sans sécurité

Le client et le serveur sont reliés par un câble croisé (RJ45) dans un environnement dit non sécuritaire, c'est-à-dire qu'aucune sécurité n'a été appliquée à cet environnement. Les usagers virtuels simulés sont au nombre de 35 pour chaque scénario de ce test. La Figure 4.9 illustre les résultats de temps de réponse dans un environnement câblé sans sécurité.

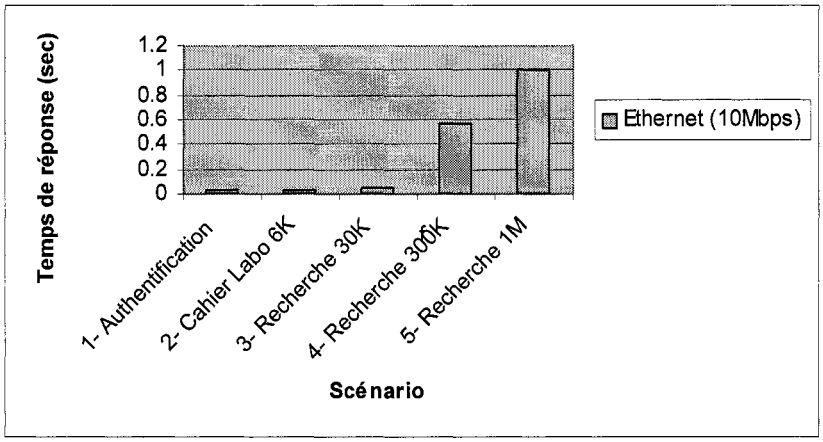

Figure 4.9 Temps de réponse Ethernet sans sécurité

Analyse des résultats : Les résultats démontrent que le temps de réponse pour chaque scénario demeure très acceptable, car l'ensemble des scénarios possède un temps de réponse inférieur à 1 seconde. Par contre, les deux derniers scénarios affichent un temps de réponse largement plus élevé que les autres. Cela est dû au fait que ces deux scénarios font des requêtes sur des fichiers volumineux. Cependant, compte tenu du fait que nous sommes dans un réseau Ethernet (10 Mbps), le temps de réponse des deux derniers scénarios n'affecte pas l'usager.

La Figure 4.10 illustre la charge du serveur lors des simulations dans l'environnement câblé sans sécurité avec 35 usagers virtuels.

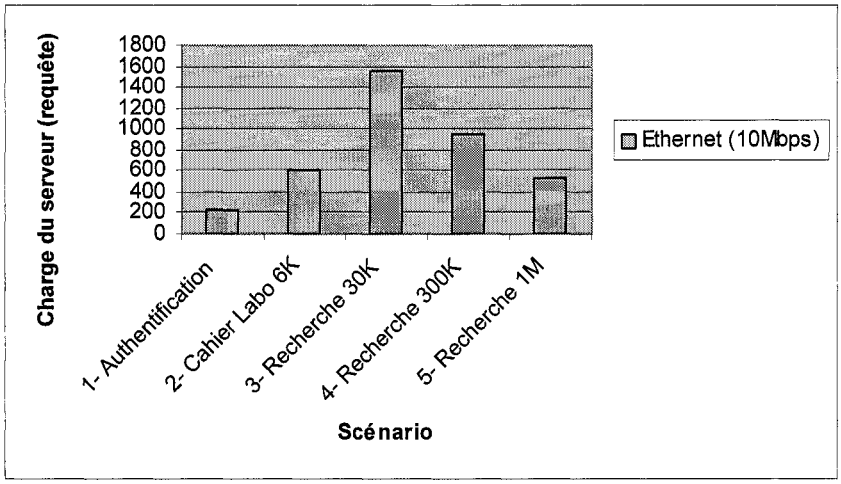

Figure 4.10 Charge du serveur Ethernet sans sécurité

Analyse des résultats : Les résultats indiquent que lors des scénarios 1 et 2, la charge du serveur est faible malgré des pages peu volumineuses. Ceci est dû au fait que, lors de ces 2 scénarios, le serveur fait une requête à la base de données. Ainsi, le serveur peut effectuer plusieurs requêtes lors du scénario 3 comprenant une recherche de 30 Ko, comparativement au scénario 2 comprenant une page et 6 Ko et un accès à la base de données. Le même principe s'applique pour le scénario 1. En effet, lors du scénario d'authentification, le serveur fait une recherche dans la base de données et compare les deux champs (nom d'usager et mot de passe), alors que dans les scénarios 3, 4 et 5, le serveur affiche uniquement une page d'information.

b) Environnement câblé avec sécurité

La Figure 4.11 présente les résultats de temps de réponse dans l'environnement câblé et sécuritaire utilisant le protocole SSL.

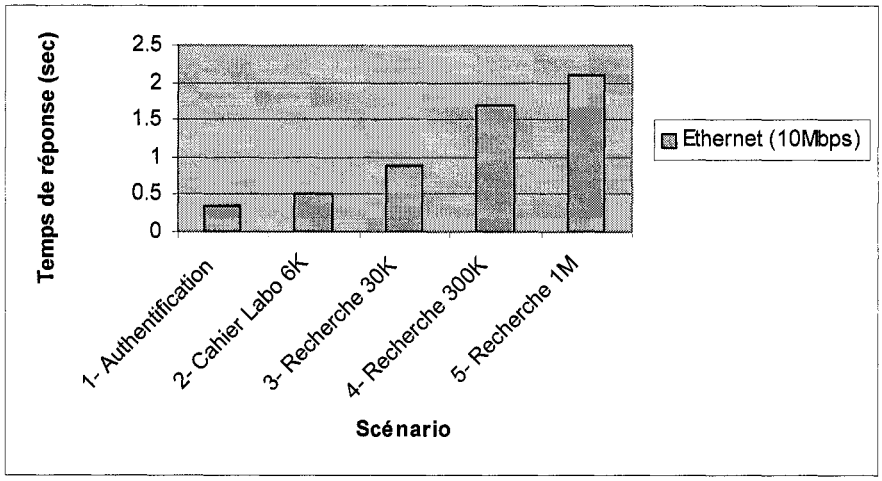

Figure 4.11 Temps de réponse Ethernet avec sécurité

Analyse des résultats : La Figure 4.11 montre que les scénarios 4 et 5 affichent un temps de réponse largement supérieur aux autres scénarios. Ceci s'explique par le gros volume des fichiers de ces deux scénarios.

La Figure 4.12 montre les résultats de la charge du serveur dans un environnement câblé et sécuritaire utilisant le protocole SSL.

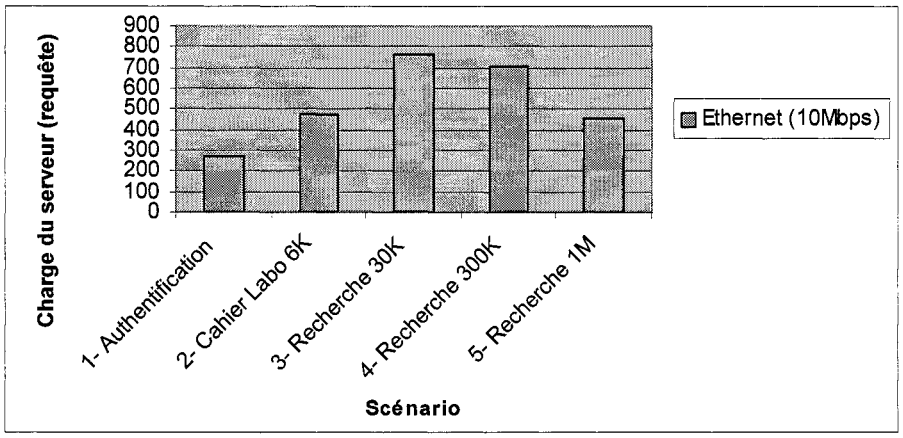

Figure 4.12 Charge du serveur Ethernet avec sécurité

Analyse des résultats : La charge de serveur demeure dans la même proportion que dans l'environnement câblé sans sécurité. Le fait d'ajouter la sécurité de type SSL diminue légèrement le nombre de requêtes auxquelles le serveur peut répondre. Ceci s'explique par l'étape de chiffrement lors de l'utilisation de SSL. Ainsi, l'ajout de SSL diminue, dans tous les scénarios, le nombre de requêtes auxquelles le serveur peut répondre dans une période donnée.

c) Environnement sans fil et sans sécurité

La Figure 4.13 illustre le temps de réponse dans un environnement WLAN (IEEE 802.11b) sans sécurité.

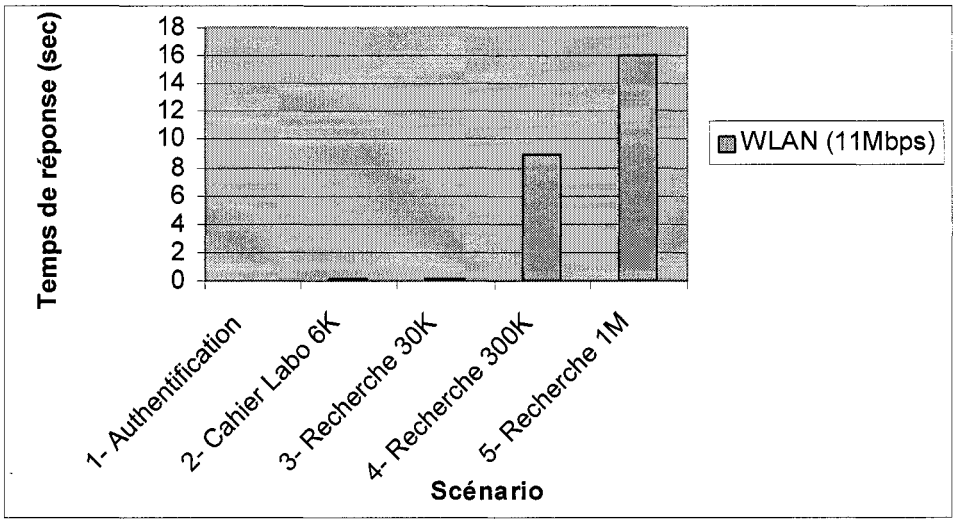

Figure 4.13 Temps de réponse WLAN sans sécurité

Analyse des résultats : Les résultats montrent que le temps de réponse pour les trois premiers scénarios est inférieur à 0.16 seconde, il est donc presqu'instantané pour l'usager. Par contre, la recherche de 300 Ko et de 1 Mo affiche un temps de réponse de 9 secondes et 16 secondes respectivement. Ceci est dû au fait que l'usager partage le réseau IEEE 802.11b avec 35 autres usagers simultanément, réduisant ainsi sa connexion à près de 314 Kbps pour chaque usager. Pour cela, nous avons mesuré le temps de réponse d'un usager dans un environnement câblé sans sécurité à 312 Kbps. Dans ce

type d'environnement, le temps de réponse pour les scénarios 4 et 5 est respectivement 9.8 seconde et 17.6 seconde. Ainsi, le temps de réponse des scénarios 4 et 5 dans l'environnement WLAN est affecté par le nombre d'usagers présents au même moment sur le réseau et est plus apparent lors de requêtes exigeant des fichiers de grande taille. La Figure 4.14 illustre la charge du serveur durant chacun des scénarios dans un environnement WLAN (IEEE 802.11b) sans sécurité.

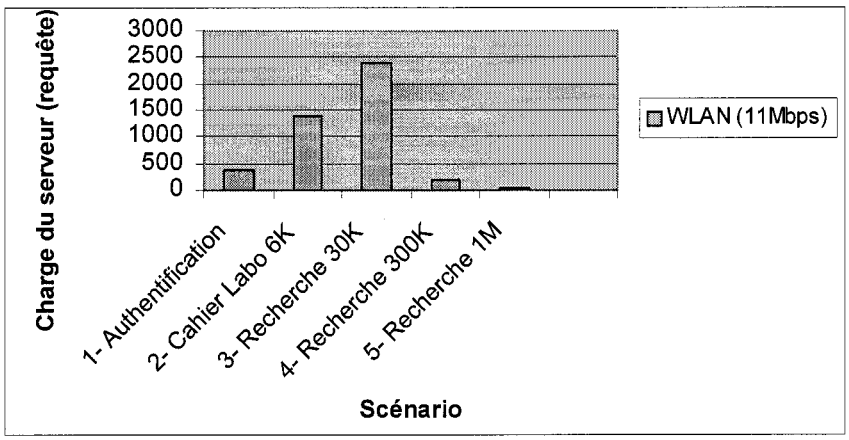

Figure 4.14 Charge du serveur WLAN sans sécurité

Analyse des résultats : Le serveur traite un grand nombre de requêtes lors du troisième scénario, alors qu'il en traite beaucoup moins lors des scénarios 4 et 5. Cela est attribué au fait que chacun des 35 usagers se partage la bande passante, devenant ainsi l'équivalent d'une bande passante de 314 Kbps pour chacun. Ainsi, le partage de la bande passante et l'exécution d'une requête de type scénario 5 font en sorte que le serveur traite beaucoup moins de requêtes comparativement aux autres scénarios. Alors, l'important volume des scénarios recherche 300 Ko et recherche 1 Mo ainsi que le partage de la bande passante font limiter le nombre de requêtes que le serveur est en mesure de traiter.

d) Environnement sans fil et avec sécurité

La Figure 4.15 présente les résultats obtenus lors de l'exécution des scénarios dans un environnement WLAN avec le mécanisme de sécurité SSL.

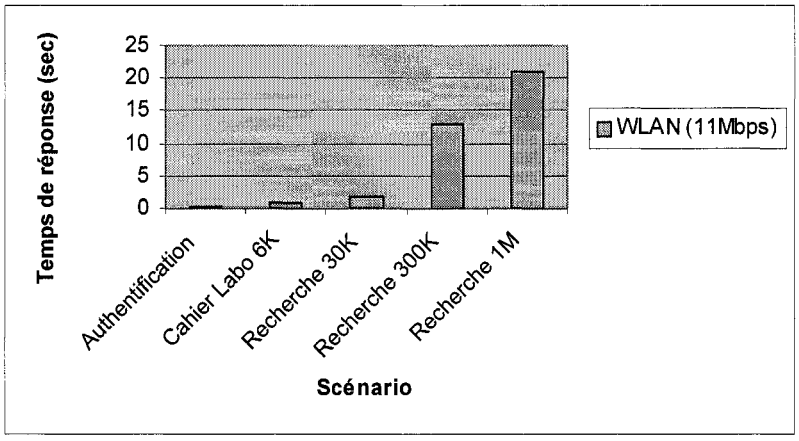

Figure 4.15 Temps de réponse WLAN avec sécurité

Analyse des résultats : Ces résultats montrent que le temps de réponse demeure dans la même proportion que le temps de réponse dans un environnement WLAN sans sécurité. Par contre, l'ajout du mécanisme de sécurité SSL augmente légèrement le temps de réponse. La Figure 4.16 illustre la charge du serveur dans un environnement WLAN (IEEE 802.11b) avec sécurité.

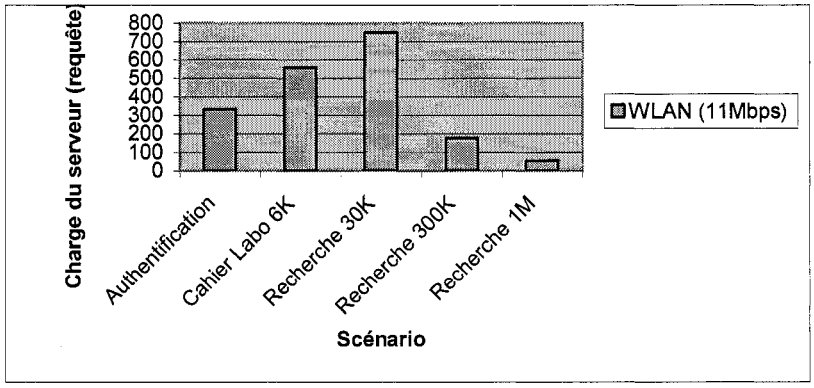

Figure 4.16 Charge du serveur WLAN avec sécurité

Analyse des résultats : Les résultats montrent que la charge du serveur demeure dans la même proportion que la charge du serveur dans l'environnement WLAN sans sécurité. Le fait d'ajouter SSL réduit le nombre de requêtes auxquelles le serveur est en mesure de répondre. Cette différence est due au chiffrement des paquets lors de l'utilisation de SSL.

Synthèse des résultats

Les temps de réponse obtenus dans l'environnement WLAN sans sécurité et ceux obtenus dans l'environnement WLAN avec sécurité sont regroupés à la Figure 4.17.

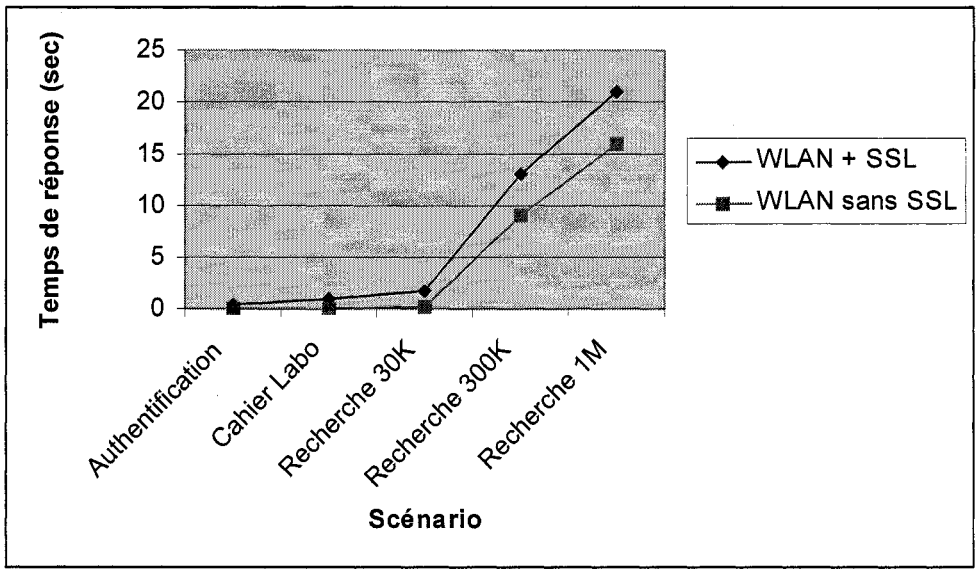

Figure 4.17 Synthèse des résultats WLAN

Les résultats montrent que, dans chacun des scénarios, l'utilisation du mécanisme de sécurité SSL n'est que légèrement plus coûteux en terme de temps de réponse que lorsque aucune sécurité n'est appliquée.

Voyons maintenant, avec la Figure 4.18, la sécurité SSL dans un environnement câblé, comparativement à un environnement mobile utilisant SSL.

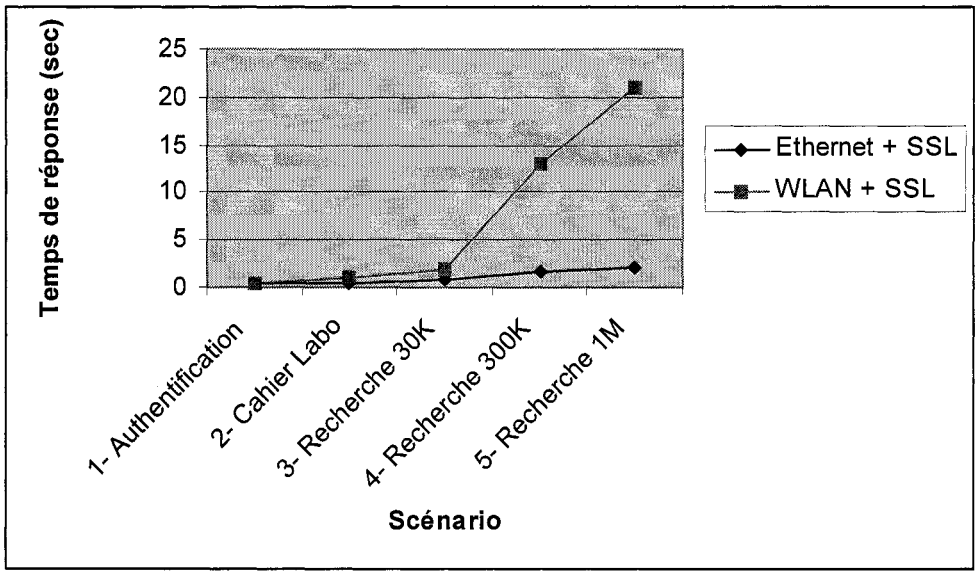

Figure 4.18 Synthèse des résultats WLAN et Ethernet utilisant SSL

Cette figure montre que, lors des trois premiers scénarios, les temps de réponse entre l'environnement fixe et mobile sont semblables. Par contre, le temps de réponse dans les scénarios 4 et 5 demeure quant à lui largement supérieur dans l'environnement mobile. Cela s'explique par le fait que la bande passante de l'environnement sans fil est partagée entre les 35 usagers, ce qui revient à 314 Kbps de bande passante pour chacun pour exécuter des requêtes très volumineuses (recherche 1 Mo). Dans l'environnement fixe Ethernet, nous utilisons un câble croisé (RJ45) qui se comporte de la même manière que si nous avions utilisé un commutateur. Dans ce cas, les usagers ne sont pas victimes des problèmes de collision, comparativement lors de l'utilisation d'un concentrateur. Ainsi, la bande passante demeure de 10 Mbps pour chaque usager.

Afin de récapituler nos analyses, nous avons inscrit tous les résultats obtenus aux tableaux 4.2 et 4.3.

Tableau 4.2 Résultats des temps de réponse en secondes

SCÉNARIOS	ETHERNET Sans SSL	ETHERNET SSL	WLAN Sans SSL	WLAN SSL
Authentification	0.034	0.36	0.05	0.45
Cahier de laboratoire	0.039	0.5	0.09	1
Recherche 30 Koctets	0.05	0.9	0.16	1.8
Recherche 300 Koctets	0.56	1.69	9	13
Recherche 1 Méga-octets	1	2.10	16	21

Tableau 4.3 Résultats de la charge du serveur en nombre de requêtes

SCÉNARIOS	ETHERNET Sans SSL	ETHERNET SSL	WLAN Sans SSL	WLAN SSL
Authentification	218	270	372	332
Cahier de laboratoire	700	470	1400	560
Recherche 30 Koctets	1557	762	2407	749
Recherche 300 Koctets	953	711	188	178
Recherche 1 Méga-octets	530	453	56	54

En observant ces résultats, nous constatons que, dans un environnement câblé (Ehternet) ou sans fil (IEEE 802.11b), le fait d'appliquer SSL sur des requêtes non volumineuses (moins de 300 Ko) augmente le temps de réponse en moyenne de 11%. Par contre, l'utilisation de SSL sur des requêtes volumineuses (plus de 300 Ko) augmente le temps de réponse en moyenne de 3%. Ainsi, l'ajout de SSL affecte

visiblement moins le temps de réponse lors de requêtes volumineuses. Ceci est dû au fait que le paquet volumineux passe la majeure partie de son temps à se déplacer sur le réseau, réduisant ainsi l'impact du chiffrement du mécanisme SSL.

CHAPITRE V
CONCLUSION

Après l'enseignement par correspondance et le *e-learning*, nous sommes maintenant dans l'ère de l'enseignement mobile, dit *m-learning*. Le principal avantage qu'offre ce type d'enseignement est la possibilité d'accéder à l'environnement d'apprentissage à n'importe quel moment et de n'importe quel endroit. Le *m-learning* implique nécessairement l'utilisation d'appareils mobiles de type PDA (Personal Digital Assistant), PocketPS ou cellulaire dans un réseau sans fil. L'utilisation de ces appareils mobiles dans les environnements d'apprentissage soulève de sérieux problèmes de sécurité et de mobilité qui n'ont jusqu'à maintenant pas été pris en compte par les environnements d'apprentissage actuel.

Le présent mémoire a porté sur le développement d'une architecture sécuritaire permettant la mobilité des terminaux, des usagers, ainsi que des services dans un environnement d'apprentissage virtuel. En guise de conclusion, nous faisons, en première partie, une synthèse de nos travaux puis nous énonçons les limitations à nos méthodes, en deuxième partie. Enfin, nous terminons ce chapitre en indiquant quelques pistes pour les travaux futurs afin de poursuivre les efforts entrepris dans cette recherche.

5.1 Synthèse des travaux

La première partie de cet ouvrage a été consacrée, à l'étude des technologies de sécurité et de mobilité. Nous avons également examiné la sécurité et la mobilité qu'offrent les environnements d'apprentissage virtuel d'aujourd'hui.

Par la suite, nous avons élaboré une architecture sécuritaire destinée à être utilisée pour les environnements d'apprentissage mobile de type laboratoire virtuel. Pour y parvenir, nous avons, tout d'abord, déterminé les composantes principales d'une telle architecture. Ensuite, nous avons posé les exigences de mobilité et de sécurité des composantes face à notre environnement. Ensuite, nous avons exploré plusieurs avenues afin de trouver une solution sécuritaire qui assurerait la mobilité dans un environnement d'apprentissage virtuel. Nous avons, par la suite, défini et décomposé chacune de ses composantes et exigences afin de formuler plusieurs cas d'utilisation pertinents à notre système suivant une modélisation UML. Ceci nous a conduit à une architecture constituée de six modules et 16 sous-modules axés sur la sécurité, tout en permettant la mobilité lors d'apprentissage. Enfin, nous avons choisi deux modules dont le module de gestion réseau ainsi que le module de sécurité manager.

Ensuite, nous avons conçu trois sections représentant l'environnement d'apprentissage : l'authentification, la recherche de cours et l'accès au cahier de laboratoire par l'étudiant. Nous avons également construit les modules de sécurité et de mobilité, puis nous les avons intégrés à notre environnement d'apprentissage. Ainsi, dans le but de mesurer la performance de notre architecture, nous avons aménagé un réseau câblé et un réseau WLAN (IEEE 802.11b).

Les étapes de conception terminées, nous avons élaboré plusieurs tests afin de mesurer la performance de notre architecture. Pour chacun des tests de performance nous avons mesuré la charge du serveur et le temps de réponse.

Les mesures du temps de réponse et la charge du réseau de chaque scénario nous ont permis de tirer les conclusion suivantes :

- Peu importe si nous utilisons le mécanisme de sécurité SSL ou non, lorsque le réseau IEEE 802.11b comporte un nombre élevé d'utilisateurs, la charge du serveur (nombre de requête) diminue. Étant donné que dans un réseau IEEE 802.11b plus le nombre d'usagers augmente plus la bande passante diminue ;

- La différence de temps de réponse entre l'utilisation de SSL et sans l'utilisation de SSL est plus élevée lors de requêtes volumineuses que lors de requêtes de faible volume ;
- Une solution SSL utilisant des requêtes à faible volume affiche les meilleurs temps ;
- L'utilisation du mécanisme de sécurité SSL augmente le temps de réponse, sur des petites requêtes (moins de 300 Ko), de 11% ;
- L'utilisation du mécanisme de sécurité SSL augmente le temps de réponse, sur des larges requêtes (plus de 300 Ko), de 3% uniquement.

Pour des connexions rapides comme Ethernet ou IEEE 802.11b, des requêtes volumineuses affichent un temps de réponse élevé. Nous devons donc éviter, dans un environnement d'apprentissage, de présenter des requêtes de grande dimension. Les résultats montrent qu'il est préférable d'offrir plusieurs pages de recherche, chacune moins de 300K, tout en assurant le mécanisme de sécurité SSL.

Ainsi, nous considérons que l'ajout de SSL dans un environnement d'apprentissage virtuel présente un coût raisonnable à payer pour assurer la sécurité.

5.2 Limitations des travaux

Parmi les limitations de nos travaux, nous pouvons noter l'absence de mécanisme de sécurité d'accès. En effet, dans un réseau WLAN axé sur l'apprentissage, il est essentiel de protéger l'accès au réseau sans toutefois restreindre la mobilité. La sécurité d'accès réseau peut influencer les performances de l'environnement d'apprentissage virtuel. Il serait donc plus vraisemblable de tester les performances avec un mécanisme de sécurité d'accès réseau.

Par ailleurs, nous avons testé le mécanisme de sécurité dans un environnement de haut débit tel que IEEE 802.11b (11 Mbps) ainsi qu'Ethernet (10 Mbps). Il serait alors intéressant d'examiner l'impact des mécanismes de sécurité dans des réseaux de plus faible débit.

5.3 Orientations de recherche futures

Ce travail nous a permis de mettre en place une architecture sécuritaire permettant la mobilité. Les mesures ont été obtenues à partir d'appareils fixes dans un réseau filiaire ainsi qu'un réseau sans fil IEEE 802.11b. Des résultats très intéressants peuvent être tirés lors de mesures sur des appareils mobiles comme le PDA, dans un réseau sans fil. Effectivement, le déplacement de l'appareil mobile tant à l'intérieur qu'à l'extérieur de la cellule peut affecter la performance des mécanismes de sécurité dans l'environnement d'apprentissage virtuel.

En dépit des résultats satisfaisants obtenus, la sécurité implémentée lors de nos tests se limite à la sécurité de l'environnement d'apprentissage virtuel. Il serait donc intéressant d'ajouter la sécurité d'accès lors de l'accès au réseau sans fil IEEE 802.11b. En effet, dans un contexte d'apprentissage mobile, le réseau doit sécuriser son accès sans restreindre la mobilité aux usagers. Les mécanismes de sécurité d'accès réseau peuvent avoir une influence sur la performance de l'environnement d'apprentissage virtuel. Enfin, l'implémentation d'un mécanisme de sécurité d'accès réseau mesuré dans un environnement sans fil avec un appareil mobile de type PDA serait une démarche pertinente et complémentaire à nos travaux.

BIBLIOGRAPHIE

Allée G., "Sécurité des agents mobiles: Protocole d'enregistrement d'itinéraire", mémoire de maîtrise génie informatique, École Polytechnique de Montréal, Canada, 2001.

Anderson D., Jassim S., "Secure and Credible e-learning Systems", *World Conference on Educational* Multimedia, *Hypermedia and Telecommunications*, Tampere, Finland, Vol.1, Juin 2001, pp. 49-50.

Barford P., Crovella M., "Generating Representative Web workloads for Network and Server Performance Evaluation", *International Conference on Measurement and Modeling of Computer Systems*, Madison, Winsconsin, July 1998, pp. 151-160.

Chalmers D., Sloman M., "A survey of quality of service in mobile computing environment", *IEEE Communications Surveys & Tutorial*, No.2, 1999, pp. 2-10.

Ciancetta M., Colomgo G., Lavagnolo R., Grillo D., "Convergence Trends for fixed and mobile services", *IEEE Personal Communications*, Vol. 6, No. 2, avril 1999, pp. 14-21.

Floch J., Hallsteinsen S., Lie A., Myrhaug H., "A reference model for context-aware mobile services", *SINTEF Telecom and Informatics*, Trondheim, Norvège, novembre 2001, No.7465, pp. 26-28.

Forman G., Sahorjan J., "The challenge of mobile computing", *IEEE Computer*, Vol. 27, No.4, avril 1994pp. 38-47.

Gang F., Zhengkun M., "Strategy of evolution toward Mobile agent-based distributed Intelligent Network", *2001 International Conferences*, Beijing , Chine, Vol.2, novembre 2001, pp 47-752.

Gupta V., Gupta S., "Securing the wireless Internet", *Communications Magazine, IEEE*, Vol. 39, No.12, décembre 2001, pp. 68-74.

Gupta V., Montenegro G., "Secure and mobile networking", *Mobility networks and application*, Vol. 3, no. 4, 1998, pp. 381-390.

Irvine C., "Quality of Security service", *New Security Paradigms Workshop*, ACM Press, Ireland, 2001, pp. 91-99.

Labiod H., "WiFi et WiFi5", *Conférence DNAC de nouvelles architectures pour les communications*, Paris, France, Vol. 2, décembre 2002, pp. 542-554.

Maamar Z., Yahyaoui H., Mansoor W., "E-Commerce through Wireless Device", *Tenth IEEE International Workshop*, Cambridge, États-Unis, juin 2001, pp. 31-36.

Min Xu, Upadhyaya S., "Secure Communication in PCs", *Vehicular Technology Conference, IEEE VTS*, Rhodes, Grèce, Vol. 3, mai 2001, pp. 2193-2197.

Mundra P., Singal T., Kamal T., "Radio frequency interference an aspect for designing a mobile radio communication system", *Vehicular Technology Conference, IEEE*, Denver, États-Unis, Vol. 2, mai 1992, pp. 860-865.

Pierre, S., "Mobile Computing and Ubiquitous Networking: Concepts, Technologies, and Challenges", *Telematics and Informatics, Elsevier Science*, Vol. 18, No. 2-3, 2001, pp.109-131.

Pierre S., "Réseaux et systèmes informatiques mobiles", Presses Internationales Polytechnique (PIP), avril 2003, pp. 5-6.

Pujolle G., "Les réseaux" , 3e edition, Eyrolle 2000, pp. 85-88.

Robert Jean-Marc, "Interface humain ordinateur spécialisées", École Polytechnique de Montréal, Cahier de notes de cours, janvier 2002.

Tapsall S., Ryan Y., "Virtual Education Institutions in Australia: Between the Idea and Reality", *in Farrell, Glen M., ed. The Development of Virtual Education: A Global Perspective. London: The Commonwealth of Learning*, 1999, pp.147-164.

Thierno Bah, "Gestion de la mobilité des services dans un environnement de téléphonie IP", mémoire de maîtrise génie informatique, École polytechnique de Montréal, Canada, 2001.

Welke, S, Roskos J., Boone J., Mayfield T., "A taxonomy of Integrity Models, Implementations, Mechanisms", *Proceedings of the 13th National Computer Security Conference*, Washington, États-Unis, octobre 1990, pp. 541-551.

RÉFÉRENCES INTERNET

1. WebCT : http://www.webct.com/
2. Merlin : http://www.hull.ac.uk/merlin/
3. Designing distributed virtual laboratories: Methodological and Telecommunications aspects : http://www.larim.polymtl.ca/publi_fichiers/CharlesLevert-IJEL.pdf
4. High Performance Computing Virtual Laboratory: http://www.hpcvl.org/
5. CSRC Computer Security Resource Center : http://csrc.nist.gov/index.html
6. Campus Network Design (Cisco) http://www.usg.edu/conferences/networking/campus_design.pdf
7. E-learning Center's : http://www.e-learningcentre.co.uk/guide2elearning/2-1/index.htm
8. RFC2002 Mobile IP : ftp://ftp.isi.edu/in-notes/rfc2002.txt
9. Réseaux de communications mobiles: http://www.prism.uvsq.fr/recherche/themes/rc2m/rcmob/
10. Sécurité des WLAN : http://www.tcom.ch/Tcom/Presentations/Wireless/SecuWLAN.pdf
11. 802.11 Security : http://www.drizzle.com/~aboba/IEEE/
12. Qualité de service dans des environnements Internet mobile : http://www-rp.lip6.fr/~legrand/These/first.pdf
13. InfoSecWriters : http://www.infosecwriters.com/
14. Leaders in e-learning Technology : http://askintl.com/index.cfm/1,0,852,4709,1510,0,html
15. Mobile computing statistic : http://www.managingchange.com/mediums/mobile/overview.htm
16. Attack on WLAN: http://www.infosecwriters.com/texts.php?op=display&id=47
17. Problématiques des architectures sécurisées: http://www.urec.cnrs.fr/securite/CNRS/vCARS/DOCUMENTS/Riguidel-int1.pdf
18. Securing wireless acces with mobile application :

http://www.webtorials.com/main/resource/papers/BCR/paper67/phifer-09-03.pdf

19. Gestion des déconnexions : http://www.lifl.fr/jc2004/slides/kouici-conan-bernard.pdf
20. Gestions des déconnexions:http://etna.int-evry.fr/~conan/Publications/dea_lynda.pdf
21. Wap Forum : http://www.wapforum.org/
22. Securité info : http://www.securiteinfo.com/conseils/choix_ids.shtml
23. Tutorial VPN : http://www.tcom.ch/Tcom/Projets/VPN/_Tutorial%20VPN.pdf
24. Andrew e-learning project : http://www.cmu.edu/computing/wireless/
25. Virtual Home Environment: keskus.hut.fi/julkaisut/tyot/erikoistyot/matkapuh/44362U.pdf
26. Qualité de service dans les environnements Internet mobile: http://www-rp.lip6.fr/~legrand/These/first.pdf
27. Qualité de service dans Internet : http://www.urec.cnrs.fr/metrologie/article-qos.html
28. Étude de Ipsos-reid : http://www.ipsos-reid.com/search/pdf/media/mr020425%2D2.pdf